ip rsvp precedence through load protocol

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

ip rsvp precedence

To enable the router to mark the IP Precedence value of the type of service (ToS) byte for packets in a Resource Reservation Protocol (RSVP) reserved path using the specified values for packets that either conform to or exceed the RSVP flowspec, use the **iprsvpprecedence**command in interface configuration mode. To remove existing IP Precedence settings, use the **no** form of this command.

ip rsvp precedence {**conform** *precedence-value* | **exceed** *precedence-value*}

no ip rsvp precedence [**conform** | **exceed**]

Syntax Description

conform *precedence-value*	Specifies an IP Precedence value in the range from 0 to 7 for traffic that conforms to the RSVP flowspec. The IP Precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified. When used with the **no** form of the command, the **conform** keyword is optional.
exceed *precedence-value*	Specifies an IP Precedence value in the range from 0 to 7 for traffic that exceeds the RSVP flowspec. The IP Precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified. When used with the **no** form of the command, the **exceed** keyword is optional.

Command Default

The IP Precedence bits of the ToS byte are left unmodified when this command is not used. The default state is equivalent to execution of the **noiprsvpprecedence** command.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Packets in an RSVP reserved path are divided into two classes: those that conform to the reservation flowspec and those that correspond to a reservation but that exceed, or are outside, the reservation flowspec.

The **iprsvpprecedence** command allows you to set the IP Precedence values to be applied to packets belonging to these two classes. You must specify the IP Precedence value for at least one class of traffic when you use this command. You can use a single instance of the command to specify values for both classes, in which case you can specify the **conform** and **exceed** keywords in either order.

As part of its input processing, RSVP uses the **iprsvpprecedence** command to set the IP Precedence bits on conforming and nonconforming packets. If per-VC DWRED is configured, the system uses the IP Precedence and ToS bit settings on the output interface in its packet drop process. The IP Precedence setting of a packet can also be used by interfaces on downstream routers.

Execution of the **iprsvpprecedence** command causes IP Precedence values for all preexisting reservations on the interface to be modified.

Note RSVP must be enabled on an interface before you can use this command; that is, use of the **iprsvpbandwidth** command must precede use of the **iprsvpprecedence** command. RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

RSVP receives packets from the underlying forwarding mechanism. Therefore, before you use the **iprsvpprecedence** command to set IP Precedence, one of the following features is required:

- Weighted fair queueing (WFQ) must be enabled on the interface.
- RSVP switched virtual circuits (SVCs) must be used.
- NetFlow must be configured to assist RSVP.

Note Use of the **no** form of this command is not equivalent to giving the **iprsvpprecedence0**command, which sets all precedence on the packets to 0, regardless of previous precedence setting.

Examples

The following example sets the IP Precedence value to 3 for all traffic on the ATM interface 0 that conforms to the RSVP flowspec and to 2 for all traffic that exceeds the flowspec:

```
interface atm0
 ip rsvp precedence conform 3 exceed 2
```

The following example sets the IP Precedence value to 2 for all traffic on ATM interface 1 that conforms to the RSVP flowspec. The IP Precedence values of those packets that exceed the flowspec are not altered in any way.

```
interface ATM1
 ip rsvp precedence conform 2
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp policy cops minimal	Lowers the COPS server’s load and improves latency times for messages on the governed router.
ip rsvp tos	Allows you to set the ToS values to be applied to packets that either conform to or exceed the RSVP flowspec.
s how ip rsvp	Displays the IP Precedence and ToS bit values to be applied to packets that either conform to or exceed the RSVP flowspec for a given interface.

ip rsvp qos

To enable Resource Reservation Protocol (RSVP) quality of service (QoS) flows on a router running Multiprotocol Label Switching traffic engineering (MPLS TE), use the **iprsvpqos** command in global configuration mode. To disable RSVP QoS flows, use the **no** form of this command.

ip rsvp qos

no ip rsvp qos

Syntax Description

This command has no arguments or keywords.

Command Default

RSVP QoS flows are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

If RSVP QoS flows and MPLS TE are enabled, the router processes and installs RSVP label switched path (LSP) and IPv4 messages such as PATH and RESV. If RSVP QoS flows and MPLS TE are then disabled with IPv4 and LSP states installed, all installed IPv4 states are immediately cleared. LSP states remain unmodified. Further refreshes or new IPv4 RSVP messages are forwarded unmodified.

Use the **showiprsvp** command to display the status of the **iprsvpqos** command.

Examples

The following example configures RSVP QoS flows on a router running MPLS TE:

```
Router> enable
Router# configure terminal
Router(config)# ip rsvp qos
```

Related Commands

Command	Description
show ip rsvp	Displays specific information for RSVP categories.

ip rsvp reservation

To enable a router to simulate receiving Resource Reservation Protocol (RSVP) RESV messages from a downstream host, use the **iprsvpreservation**command in global configuration mode. To disable this function, use the **no** form of this command.

ip rsvp reservation *session-ip-address sender-ip-address* {*ip-protocol* | **tcp** | **udp**} *session-dest-port sender-source-port next-hop-address next-hop-interface* {**ff** | **se** | **wf**} {**load** | **rate**} *bandwidth burst-size* [**identity** *alias*]

no ip rsvp reservation *session-ip-address sender-ip-address* {*ip-protocol* | **tcp** | **udp**} *session-dest-port sender-source-port next-hop-address next-hop-interface* {**ff** | **se** | **wf**} {**load** | **rate**} *bandwidth burst-size* [**identity** *alias*]

Syntax Description

session-ip-address	For unicast sessions, the address of the intended receiver; for multicast sessions, the IP multicast address of the session.
sender-ip-address	IP address of the sender.
ip-protocol |**tcp** | **udp**	Specifies the IP protocol in the range of 0 to 255, TCP, or UDP.
session-dest-port sender-source-port	*The session-dest-port* argument is the destination port. The *sender-source-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero (except for Wildcard Filterreservations, for which the source port is always ignored and can therefore be zero).
next-hop-address	Hostname or IP address of the receiver or the router closest to the receiver.
next-hop-interface	Next-hop interface or subinterface type and number. Interface type can be **ethernet**, **loopback**, **null**, or **serial**.
ff | **se** | **wf**	Specifies the reservation style: • **ff--** Fixed Filter with single reservation. • **se** --Shared Explicit with shared reservation and limited scope. • **wf** --Wildcard Filter with shared reservation and unlimited scope.

load	Specifies the controlled load service.
rate	Specifies the Quality of Service (QoS) guaranteed bit rate service.
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (kbps of data in queue). The range is from 1 to 65535.
identity alias	(Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable characters (in the range 0x20 to 0x7E). **Note** If you use the “ ” or ? character as part of the alias or locator string itself, you must type the CTRL-V key sequence before entering the embedded “ ” or ? character. The alias is never transmitted to other routers.

Command Default

The router does not simulate receiving RSVP RESV messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.4(6)T	This command was modified. The optional**identity***alias* keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use the **iprsvpreservation** command to make the router simulate receiving RSVP RESV messages from a downstream host and to proxy RSVP RESV messages for that host. By giving a local (loopback) next-hop address and next-hop interface, you can also use this command to proxy RSVP for the router that you are configuring or you can use the **iprsvpreservation-host** command.

An alias must reference an RSVP identity that you created by using the **iprsvpidentity** command. The policy-locator string associated with this identity is signaled in the RESV message. This identity overrides any application ID that is contained in the matching PATH message.

If the matching PATH message has an application ID, but you have not specified an application ID using the **iprsvpreservation** command, the RESV message will not contain an application ID. However, the RESV message proxied by the **iprsvplistener** command does put the matching PATH message application ID into the proxied RESV message.

Examples

The following example specifies the use of a Shared Explicit style of reservation and the controlled load service, with token buckets of 100 or 150 kbps and a maximum queue depth of 60 or 65 kbps:

```
Router(config)# ip rsvp reservation 192.168.0.2 172.16.1.1 udp 20 30 172.16.4.1 Ethernet1
se load 100 60
Router(config)# ip rsvp reservation 192.168.0.2 172.16.2.1 tcp 20 30 172.16.4.1 Ethernet1
se load 150 65
```

The following example specifies the use of a Wildcard Filter style of reservation and the guaranteed bit rate service, with token buckets of 300 or 350 kbps, a maximum queue depth of 60 or 65 kbps, and an application ID:

```
Router(config)# ip rsvp reservation 192.168.0.3 0.0.0.0 udp 20 0 172.16.4.1 Ethernet1 wf
rate 300 60 identity xyz
Router(config)# ip rsvp reservation 192.168.1.1 0.0.0.0 udp 20 0 172.16.4.1 Ethernet1 wf
rate 350 65 identity xyz
```

Note that the wildcard filter does not admit the specification of the sender; it accepts all senders. This action is denoted by setting the source address and port to zero. If, in any filter style, the destination port is specified to be zero, RSVP does not permit the source port to be anything else; it understands that such protocols do not use ports or that the specification applies to all ports.

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp identity	Defines RSVP application IDs.
ip rsvp neighbor	Enables a router to control who its authorized neighbors are.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving RSVP PATH messages.
ip rsvp sender-host	Enables a router to simulate a host generating RSVP PATH messages.

Command	Description
show ip rsvp installed	Displays RSVP-related bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp policy identity	Displays selected RSVP identities in a router configuration.
show ip rsvp reservation	Displays RSVP RESV-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp reservation-host

To enable a router to simulate a host generating Resource Reservation Protocol (RSVP) RESV messages, use the **iprsvpreservation-host**command in global configuration mode. To disable this function, use the **no** form of this command.

ip rsvp reservation-host *session-ip-address sender-ip-address* {*ip-protocol* | **tcp** | **udp**} *session-dest-port sender-source-port* {**ff** | **se** | **wf**} {**load** | **rate**} *bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]

no ip rsvp reservation-host *session-ip-address sender-ip-address* {*ip-protocol* | **tcp** | **udp**} *session-dest-port sender-source-port* {**ff** | **se** | **wf**} {**load** | **rate**} *bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver. IP multicast addresses cannot be used with this argument. It must be a logical address configured on an interface on the router that you are configuring.
sender-ip-address	IP address of the sender.
ip-protocol | **tcp** | **udp**	Specifies the IP protocol in the range of 0 to 255, TCP or UDP.
session-dest-port sender-source-port	*The session-dest-port* argument is the destination port. The *sender-source-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero (except for Wildcard Filter reservations, for which the source port is always ignored and can therefore be zero).
ff | **se** | **wf**	Specifies the reservation style: • **ff--** Fixed Filter with single reservation. • **se** --Shared Explicit with shared reservation and limited scope. • **wf** --Wildcard Filter with shared reservation and unlimited scope.
load	Specifies the controlled load service.
rate	Specifies the Quality of Service (QoS) guaranteed bit rate service.

bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (kbps of data in queue). The range is from 1 to 65535.
identity alias	(Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable characters (in the range 0x20 to 0x7E). **Note** If you use the “ ” or ? character as part of the alias or locator string itself, you must type the CTRL-V key sequence before entering the embedded “ ” or ? character. The alias is never transmitted to other routers.
vrf vrf-name	(Optional) Specifies a virtual routing and forwarding (VRF) instance.

Command Default

The router does not simulate a host generating RSVP RESV messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	This command was introduced.
12.4(6)T	This command was modified. The optional**identity***alias* keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. The optional **vrf***vrf-name* keyword and argument combination was added.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Note The syntax of the command depends on your platform and release. The **vrf***vrf-name*keyword and argument combination is not supported on ASR 1000 Series Aggregation Services Routers.

Use the **iprsvpreservation-host**command to make a router simulate a host generating its own RSVP RESV messages. This command is similar to the **iprsvpreservation** command, which can cause a router to generate RESV messages on behalf of another host. The main differences between the **iprsvpreservation-host** and **iprsvpreservation** commands follow:

- When you enter the **iprsvpreservation-host** command, the *session-ip-address* argument must be a local address configured on an interface on the router. Therefore, you cannot proxy a reservation on behalf of a flow that is destined for another host. Also, you cannot use this command to generate reservation messages for multicast sessions.
- Because the message is assumed to originate from the router that you are configuring, you do not specify a next-hop or incoming interface for the RSVP RESV message when entering the **iprsvpreservation-host** command.
- Use the **iprsvpreservation-host** command for debugging and testing purposes because you cannot use it to proxy RSVP for non-RSVP-capable hosts or for multicast sessions.

An alias must reference an RSVP identity that you created by using the **iprsvpidentity** command. The policy-locator string associated with this identity is signaled in the RESV message. This identity overrides any application ID that is contained in the matching PATH message.

If the matching PATH message has an application ID, but you have not specified an application ID using the **iprsvpreservation-host** command, the RESV message does not contain an application ID. However, the RESV message proxied by the **iprsvplistener** command does put the matching PATH message application ID into the proxied RESV message.

Examples

The following example specifies the use of a Shared Explicit style of reservation and the controlled load service, with token buckets of 100 or 150 kbps, 60 or 65 kbps maximum queue depth, and an application ID:

```
Router(config)# ip rsvp reservation-host 10.1.1.1 10.30.1.4 udp 20 30 se load 100 60
identity xyz
Router(config)# ip rsvp reservation-host 10.40.2.2 10.22.1.1 tcp 20 30 se load 150 65
identity xyz
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp identity	Defines RSVP application IDs.
ip rsvp neighbor	Enables a router to control who its authorized RSVP neighbors are.
ip rsvp reservation	Enables a router to simulate receiving RSVP RESV messages.

Command	Description
ip rsvp sender	Enables a router to simulate receiving RSVP PATH messages.
ip rsvp sender-host	Enables a router to simulate a host generating RSVP PATH messages.
show ip rsvp installed	Displays RSVP-related bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp policy identity	Displays selected RSVP identities in a router configuration.
show ip rsvp reservation	Displays RSVP RESV-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp resource-provider

To configure a resource provider for an aggregate flow, use the **iprsvpresource-provider** command in interface configuration mode. To disable a resource provider for an aggregate flow, use the **no** form of this command.

ip rsvp resource-provider {**none** | **wfq interface** | **wfq pvc**}

no ip rsvp resource-provider

Syntax Description

none	Specifies no resource provider regardless of whether one is configured on the interface.
wfq interface	Specifies Weighted fair queueing (WFQ) as the resource provider on the interface.
wfq pvc	Specifies WFQ as the resource provider on the permanent virtual circuit (PVC) or connection.

Command Default

WFQ (the **wfqinterface**keyword) is the default resource provider that Resource Reservation Protocol (RSVP) configures on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXF2	This command was integrated into Cisco IOS Release 12.2(18)SXF2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Note The syntax of the command depends on your platform and image. The **wfqinterface** and **wfqpvc** keywords are not supported on Cisco ASR 1000 series routers.

Use the **iprsvpresource-provider** command to configure the resource provider with which you want RSVP to interact when it installs a reservation.

To ensure that a flow receives quality of service (QoS) guarantees when using WFQ on a per-flow basis, configure **wfqinterface** or **wfqpvc** as the resource provider. To ensure that a flow receives QoS guarantees when using class-based weighted fair queueing (CBWFQ) for data packet processing, configure**none** as the resource provider.

Note Resource provider was formerly called QoS provider.

Examples

In the following example, the **iprsvpresource-provider** command is configured with **wfqpvc** as the resource provider, ensuring that a flow receives QoS guarantees when using WFQ on a per-flow basis:

```
Router# configure terminal
Router(config)# interface atm 6/0
Router(config-if)# ip rsvp resource-provider wfq pvc
```

In the following example, the **iprsvpresource-provider** command is configured with **none**as the resource provider, ensuring that a flow receives QoS guarantees when using CBWFQ for data-packet processing:

```
Router# configure terminal
Router(config)# interface atm 6/0
Router(config-if)# ip rsvp resource-provider none
```

Related Commands

Command	Description
show ip rsvp interface	Displays RSVP-related interface information.

ip rsvp sender

To enable a router to simulate receiving Resource Reservation Protocol (RSVP) PATH messages, use the **iprsvpsender**command in global configuration mode. To disable this function, use the **no** form of this command.

ip rsvp sender *session-ip-address sender-ip-address* {*ip-protocol* | **tcp** | **udp**} *session-dest-port sender-source-port previous-hop-ip-address previous-hop-interface bandwidth burst-size* [**identity** *alias*]

no ip rsvp sender *session-ip-address sender-ip-address* {*ip-protocol* | **tcp** | **udp**} *session-dest-port sender-source-port previous-hop-ip-address previous-hop-interface bandwidth burst-size* [**identity** *alias*]

Syntax Description

session-ip-address	For unicast sessions, the address of the intended receiver; for multicast sessions, the IP multicast address of the session.
sender-ip-address	IP address of the sender.
ip-protocol | **tcp** | **udp**	Specifies the IP protocol in the range of 0 to 255, TCP or UDP.
session-dest-port sender-source-port	*The session-dest-port* argument is the destination port. The *sender-source-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero.
previous-hop-ip-address	Address of the sender or the router closest to the sender.
previous-hop-interface	Previous-hop interface or subinterface. Interface type can be **ethernet**, **gigabitethernet**, **loopback**, **null**, or **serial**.
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (kbps of data in queue). The range is from 1 to 65535.

identity *alias*	(Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable character (in the range 0x20 to 0x7E). **Note** If you use the “ ” or ? character as part of the alias or locator string itself, you must type the CTRL-V key sequence before entering the embedded “ ” or ? character. The alias is never transmitted to other routers.

Command Default

The router does not simulate receiving RSVP PATH messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.4(6)T	This command was modified. The optional **identity***alias*keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use the **iprsvpsender** command to make the router simulate the receiving of RSVP PATH messages from an upstream host and to proxy RSVP PATH messages from that host. By including a local (loopback) previous-hop address and previous-hop interface, you can also use this command to proxy RSVP for the router that you are configuring.

An alias must reference an RSVP identity that you created by using the **iprsvpidentity** command. The policy-locator string associated with this identity is supplied in the PATH message.

Examples

The following example sets up the router to act as though it is receiving RSVP PATH messages using UDP over loopback interface 1:

```
Router(config)# ip rsvp sender 192.168.0.1 172.16.2.1 udp 20 30 172.16.2.1 loopback1 50 5
identity xyz
Router(config)# ip rsvp sender 192.168.0.2 172.16.2.1 udp 20 30 172.16.2.1 loopback1 50 5
identity xyz
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp identity	Defines RSVP application IDs.
ip rsvp neighbor	Enables a router to control who its authorized RSVP neighbors are.
ip rsvp reservation	Enables a router to simulate receiving RSVP RESV messages.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender-host	Enables a router to simulate a host generating RSVP PATH messages.
show ip rsvp installed	Displays RSVP-related bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp policy identity	Displays selected RSVP identities in a router configuration.
show ip rsvp reservation	Displays RSVP RESV-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp sender-host

To enable a router to simulate a host generating a Resource Reservation Protocol (RSVP) PATH message, use the **iprsvpsender-host**command in global configuration mode. To disable this function, use the **no** form of this command.

ip rsvp sender-host *session-ip-address sender-ip-address* {*ip-protocol* | **tcp** | **udp**} *session-dest-port sender-source-port bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]

no ip rsvp sender-host *session-ip-address sender-ip-address* {*ip-protocol* | **tcp** | **udp**} *session-dest-port sender-source-port bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]

Syntax Description

session-ip-address	For unicast sessions, the address of the intended receiver; for multicast sessions, the IP multicast address of the session.
sender-ip-address	IP address of the sender. It must be a logical address configured on an interface on the router that you are configuring.
ip-protocol |**tcp** | **udp**	Specifies the IP protocol in the range of 0 to 255, TCP or UDP.
session-dest-port sender-source-port	*The session-dest-port* argument is the destination port. The *sender-source-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero.
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (kbps of data in queue). The range is from 1 to 65535.
identity *alias*	(Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable characters (in the range 0x20 to 0x7E). **Note** If you use the “ ” or ? character as part of the string itself, you must type the CTRL-V key sequence before entering the embedded “ ” or ? character. The alias is never transmitted to other routers.

vrf vrf-name	(Optional) Specifies a virtual routing and forwarding (VRF) instance.

Command Default

The router does not simulate RSVP PATH message generation.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	This command was introduced.
12.4(6)T	This command was modified. The optional **identity***alias*keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. The optional **vrf***vrf-name* keyword and argument combination was added.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Note The syntax of the command depends on your platform and release. The **vrf***vrf-name*keyword and argument combination is not supported on ASR 1000 Series Aggregation Services Routers.

Use the **iprsvpsender-host**command to make a router simulate a host generating its own RSVP PATH messages. This command is similar to the **iprsvpsender** command, which can cause a router to generate RSVP PATH messages on behalf of another host. The main differences between the **iprsvpsender-host** and **iprsvpsender** commands follow:

- When you enter the **iprsvpsender-host** command, the *sender-ip-address* argument must be a local address configured on an interface of the router.
- Because the message is assumed to originate from the router that you are configuring, you do not specify a previous-hop or incoming interface for the RSVP PATH message when entering the **iprsvpsender-host** command.

- Use the **iprsvpsender-host** command for debugging and testing purposes because you cannot use it to proxy RSVP for non-RSVP-capable hosts.

An alias must reference an RSVP identity that you created by using the **iprsvpidentity** command. The policy-locator string associated with this identity is signaled in the RESV message. This identity overrides any application ID that is contained in the matching PATH message.

Examples

The following example sets up the router to act like a host that sends traffic to the given address:

```
Router(config)# ip rsvp sender-host 10.0.0.7 10.0.0.1 udp 1 1 10 10 identity xyz
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp identity	Defines RSVP application IDs.
ip rsvp neighbor	Enables a router to control who its authorized neighbors are.
ip rsvp reservation	Enables a router to simulate receiving RSVP RESV messages.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving RSVP PATH messages.
show ip rsvp installed	Displays RSVP-related bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp policy identity	Displays selected RSVP identities in a router configuration.
show ip rsvp reservation	Displays RSVP RESV-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp signalling dscp

To specify the differentiated services code point (DSCP) value to be used on all Resource Reservation Protocol (RSVP) messages transmitted on an interface, use the **iprsvpsignallingdscp** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip rsvp signalling dscp *value*

no ip rsvp signalling dscp

Syntax Description

value	A number for the DSCP. Range is from 0 to 63. Default is 0.

Command Default

The default value is 0.

Command Modes

Interface configuration.

Command History

Release	Modification
12.1	This command was introduced
12.2(18)SXF2	This command was integrated into Cisco IOS Release 12.2(18)SXF2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You configure the DSCP per interface, not per flow. The DSCP determines the priority that a packet receives from various hops as it travels to its destination.

The DSCP applies to all RSVP flows installed on a specific interface. You can configure each interface independently for DSCP.

Examples

Here is an example of the **iprsvpsignallingdscp**command with a DSCP value of 6

```
Router(config-if)# ip rsvp signalling dscp 6
Router(config-if)# end
```

To verify the DSCP value, enter the **showiprsvpinterfacedetail** command:

```
Router# show ip rsvp interface serial2/0 detail
```

```
Se2/0:
   Bandwidth:
     Curr allocated:10K bits/sec
     Max. allowed (total):1536K bits/sec
     Max. allowed (per flow):1536K bits/sec
   Neighbors:
     Using IP enacp:1.  Using UDP encaps:0
   DSCP value used in Path/Resv msgs:0x6
   Burst Police Factor:300%
   RSVP:Data Packet Classification provided by: none
```

ip rsvp signalling fast-local-repair notifications

To configure the number of per flow notifications that Resource Reservation Protocol (RSVP) processes during a fast local repair (FLR) procedure before suspending, use the **iprsvpsignallingfast-local-repairnotifications** command in global configuration mode. To set the number of notifications to its default, use the **no** form of this command.

ip rsvp signalling fast-local-repair notifications *number*

no ip rsvp signalling fast-local-repair notifications

Syntax Description

number	Total number of notifications to be sent. The range is from 10 to 10000. The default value is 1000.

Command Default

Notifications are sent by the Routing Information Base (RIB) and processed by RSVP. If the **iprsvpsignallingfast-local-repairnotifications** command is not configured, RSVP processes 1000 notifications, suspends the notifications, and then resumes processing of another 1000 notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Upon a route change, RIB builds a list of notifications, one per affected flow, and notifies RSVP by sending an event including these notifications. Therefore, these events can contain thousands of elements, depending on the number of path state blocks (PSBs) affected.

RSVP processes, by default, 1000 notifications at a time and then suspends if required, to prevent the CPU from being overwhelmed. However, you can configure this number using the **iprsvpsignallingfast-local-repairnotifications** command.

Examples

The following example shows how to configure the number of flows that are repaired before RSVP suspends to 100:

```
Router(config)# ip rsvp signalling fast-local-repair notifications 100
```

Related Commands

Command	Description
ip rsvp signalling fast-local-repair rate	Configures the repair rate that RSVP uses for an FLR procedure.
ip rsvp signalling fast-local-repair wait-time	Configures the delay that RSVP uses to start an FLR procedure.
show ip rsvp signalling fast-local-repair	Displays FLR-specific information maintained by RSVP.

ip rsvp signalling fast-local-repair rate

To configure the repair rate that Resource Reservation Protocol (RSVP) uses for a fast local repair (FLR) procedure, use the **iprsvpsignallingfast-local-repairrate**command in global configuration mode. To set the repair rate to its default, use the **no** form of this command.

ip rsvp signalling fast-local-repair rate *messages-per-second*

no ip rsvp signalling fast-local-repair rate

Syntax Description

messages-per-second	FLR rate for PATH state refresh and repair, in messages per second. The range is 1 to 2500. The default is 400.

Command Default

If this command is not configured, the RSVP message pacing rate is used.

Note

The RSVP message pacing rate is enabled by default in Cisco IOS Release 12.2 and later releases.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

The default repair rate is based on the RSVP message pacing rate.

If you configure the FLR rate by using the **iprsvpsignallingfast-local-repairrate** command, and RSVP message pacing is enabled, the lower FLR rate and the RSVP message pacing rate takes effect. If you disable the RSVP rate limit by using the**noiprsvpsignallingrate-limit**command, then the FLR rate is used. However, if you disable the RSVP rate limit and do not configure an FLR rate, then RSVP performs no message pacing and messages are sent back-to-back. This action is not recommended because the point of local repair (PLR) may flood the downstream node with PATH messages causing some of them to be dropped.

The repair rate is determined at notification time, and this same rate is used during the time of the repair even if you change either the RSVP message pacing rate or the FLR rate during this time.

Examples

The following example shows how to configure a repair rate of 100 messages per second:

```
Router(config)# ip rsvp signalling fast-local-repair rate 100
```

Related Commands

Command	Description
ip rsvp signalling fast-local-repair notifications	Configures the number of notifications that are processed before RSVP suspends.
ip rsvp signalling fast-local-repair wait-time	Configures the delay used to start an FLR procedure.
ip rsvp signalling rate-limit	Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time.

ip rsvp signalling fast-local-repair wait-time

To configure the delay that Resource Reservation Protocol (RSVP) uses before starting a fast local repair (FLR) procedure, use the **iprsvpsignallingfast-local-repairwait-time**command in interface configuration mode. To set the delay to its default, use the **no** form of this command.

ip rsvp signalling fast-local-repair wait-time *interval*

no ip rsvp signalling fast-local-repair wait-time

Syntax Description

interval	Amount of time before an FLR procedure begins, in milliseconds (ms). The range is 0 to 5000. The default is 0.

Command Default

This command is disabled by default; therefore, no delay is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use the **iprsvpsignallingfast-local-repairwait-time** command to configure the delay desired in starting an FLR procedure. If you do not configure a delay, then path refreshes are triggered immediately after RSVP receives a route change notification from the Routing Information Base (RIB).

Examples

The following example configures a delay of 100 ms:

```
Router(config-if)# ip rsvp signalling fast-local-repair wait-time 100
```

Related Commands

Command	Description
ip rsvp signalling fast-local-repair notifications	Configures the number of notifications that are processed before RSVP suspends.
ip rsvp signalling fast-local-repair rate	Configures the repair rate that RSVP uses for an FLR procedure.

ip rsvp signalling hello (configuration)

To enable Hello globally on the router, use the **iprsvpsignallinghello**command in global configuration mode. To disable Hello globally on the router, use the **no** form of this command.

ip rsvp signalling hello

no ip rsvp signalling hello

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

To enable Hello globally on the router, you must enter this command. You also must enable Hello on the interface.

Examples

In the following example, Hello is enabled globally on the router:

```
Router(config)# ip rsvp signalling hello
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.

ip rsvp signalling hello (interface)

To enable hello on an interface where you need Fast Reroute protection, use the **iprsvpsignallinghello**command in interface configuration mode. To disable hello on an interface where you need Fast Reroute protection, use the **no** form of this command

ip rsvp signalling hello

no ip rsvp signalling hello

Syntax Description

This command has no arguments or keywords.

Command Default

No hellos are enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You must configure hello globally on a router and on the specific interface.

Examples

In the following example, hello is enabled on an interface:

```
Router(config-if)# ip rsvp signalling hello
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello dscp	Sets the DSCP value that is in the IP header of the Hello messages sent out from the interface.
ip rsvp signalling hello refresh misses	Specifies how many Hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.
ip rsvp signalling hello refresh interval	Configures the Hello request interval.

ip rsvp signalling hello dscp

To set the differentiated services code point (DSCP) value that is in the IP header of a Resource Reservation Protocol (RSVP) traffic engineering (TE) hello message sent from an interface, use the **iprsvpsignallinghellodscp** command in interface configuration mode. To set the DSCP value to its default, use the **no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **dscp** *num*

no ip rsvp signalling hello [**fast-reroute**] **dscp**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
num	DSCP value. Valid values are from 0 to 63.

Command Default

The default DSCP value is 48.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute** keyword was added.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If a link is congested, it is recommended that you set the DSCP to a value higher than 0 to reduce the likelihood that hello messages will be dropped.

You configure the DSCP per interface, not per flow.

The DSCP applies to the RSVP hellos created on a specific interface. You can configure each interface independently for DSCP.

If you issue the **iprsvpsignallinghellodscp** command without the optional **fast-reroute**keyword, the command applies to Fast Reroute hellos. This command is provided for backward compatibility; however, we recommend that you use the **iprsvpsignallinghellofast-reroutedscp**command.

Examples

In the following example, hello messages sent from this interface have a DSCP value of 30 and Fast Reroute capability is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute dscp 30
```

In the following example, hello messages sent from this interface have a DSCP value of 30 and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello dscp 30
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables hellos on an interface where you need Fast Reroute protection.
ip rsvp signalling hello refresh interval	Sets the hello refresh interval in hello messages.
ip rsvp signalling hello reroute refresh misses	Sets the missed refresh limit in hello messages.

ip rsvp signalling hello graceful-restart

To enable the Resource Reservation protocol (RSVP) traffic engineering (TE) graceful restart capability on a neighboring router, use the **iprsvpsignallinghellograceful-restart** command in interface configuration mode. To disable the graceful restart capability, use the **no** form of this command.

ip rsvp signalling hello graceful-restart

no ip rsvp signalling hello graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Default

Neighboring routers have only node hello enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use the **iprsvpsignallinghellograceful-restart** command to enable support for graceful restart on routers helping their neighbors recover TE tunnels following stateful switchover (SSO).

Note This command is optional. Use it when node hello is not supported.

Examples

The following example configures graceful restart on POS interface 1/0/0 of a neighboring router with the IP address 10.0.0.1:

```
Router# configure terminal

Enter configuration commands, one per line. End with CTTL/Z.
Router(config)# interface POS1/0/0

Router(config-if)# ip rsvp signalling hello graceful-restart
```

Related Commands

Command	Description
ip rsvp signalling hello graceful-restart mode	Enables RSVP TE graceful restart support capability on an RP, and enables node hello.
show ip rsvp hello graceful-restart	Displays information about RSVP TE graceful restart hello messages.

ip rsvp signalling hello graceful-restart dscp

To set the differentiated services code point (DSCP) value that is in the IP header of a Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart hello message, use the **iprsvpsignallinghellograceful-restartdscp** command in global configuration mode. To set the DSCP valueto its default, use the **no** form of this command.

ip rsvp signalling hello graceful-restart dscp *num*

no ip rsvp signalling hello graceful-restart dscp

Syntax Description

num	DSCP value. Valid values are from 0 to 63.

Command Default

The default DSCP value is 48.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If a link is congested, set the DSCP to a value higher than 0 to reduce the likelihood that hello messages get dropped.

The DSCP applies to the RSVP hellos created on a specific router. You can configure each router independently for the DSCP.

Examples

In the following example, hello messages have a DSCP value of 30:

```
Router(config)# ip rsvp signalling hello graceful-restart dscp 30
```

Related Commands

Command	Description
ip rsvp signalling hello graceful-restart refresh interval	Sets the hello request interval in graceful restart hello messages.
ip rsvp signalling hello graceful-restart refresh misses	Sets the missed refresh limit in graceful restart hello messages.

ip rsvp signalling hello graceful-restart mode

To enable Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart capability on a Route Processor (RP), use the **iprsvpsignallinghellograceful-restartmode**command in global configuration mode. To disable graceful restart capability, use the **no** form of this command.

Cisco IOS 12.0(29)S, 12.2(33)SRA, 12.2(33)SXH, and Later Releases

ip rsvp signalling hello graceful-restart mode {**help-neighbor** | **full**}

no ip rsvp signalling hello graceful-restart mode

Cisco IOS T and XE Trains

ip rsvp signalling hello graceful-restart mode help-neighbor

no ip rsvp signalling hello graceful-restart mode help-neighbor

Syntax Description

help-neighbor	Enables support for a neighboring router to restart after a failure.
full	Enables support for a router to perform self-recovery or to help a neighbor restart after a failure.

Command Default

Graceful restart is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(29)S	This command was introduced as **iprsvpsignallinghellograceful-restartmodehelp-neighbor**.
12.2(33)SRA	This command was modified. The **full** keyword was added.This command replaces the as **iprsvpsignallinghellograceful-restartmodehelp-neighbor**command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Release	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **iprsvpsignallinghellograceful-restartmodehelp-neighbor**command to enable support capability for a neighboring router to restart after a failure.

Use the **iprsvpsignallinghellograceful-restartmodefull**command to enable support capability for a router to begin self-recovery or help its neighbor to restart on platforms that support stateful switchover (SSO), such as Cisco 7600 series routers, provided that you have installed and configured a standby RP.

Examples

The following example shows how to configure an RP with support capability to perform self-recovery after a failure:

```
Router(config)# ip rsvp signalling hello graceful-restart mode full
```

Related Commands

Command	Description
ip rsvp signalling hello graceful-restart dscp	Sets the DSCP value in the IP header of a RSVP TE graceful restart hello message.
ip rsvp signalling hello graceful-restart neighbor	Enables RSVP-TE graceful restart support capability on a neighboring router.
ip rsvp signalling hello graceful-restart refresh interval	Sets the value to control the request interval in graceful restart hello messages.
ip rsvp signalling hello graceful-restart refresh misses	Sets the value to control the missed refresh limit in graceful restart hello messages.
show ip rsvp hello graceful-restart	Displays information about RSVP-TE graceful restart hello messages.

ip rsvp signalling hello graceful-restart mode help-neighbor

Note Effective with Cisco IOS Release 12.2(33)SRA, the **iprsvpsignallinghellograceful-restartmodehelp-neighbor** command is replaced by the **iprsvpsignallinghellograceful-restartmode**command. See the **iprsvpsignallinghellograceful-restartmode**command for more information.

To enable Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart capability on a neighboring router, use the **iprsvpsignallinghellograceful-restartmodehelp-neighbor**command in global configuration mode. To disable graceful restart capability, use the **no** form of this command.

ip rsvp signalling hello graceful-restart mode help-neighbor

no ip rsvp signalling hello graceful-restart mode help-neighbor

Syntax Description

This command has no arguments or keywords.

Command Default

Graceful restart is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was replaced by the **iprsvpsignallinghellograceful-restartmode**command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **iprsvpsignallinghellograceful-restartmodehelp-neighbor** command to restart a neighboring router.

Examples

In the following example, graceful restart is enabled:

```
Router(config)# ip rsvp signalling hello graceful-restart mode help-neighbor
```

Related Commands

Command	Description
ip rsvp signalling hello graceful-restart dscp	Sets the DSCP value in the IP header of a RSVP TE graceful restart hello message.
ip rsvp signalling hello graceful-restart refresh interval	Sets the value to control the request interval in graceful restart hello messages.
ip rsvp signalling hello graceful-restart refresh misses	Sets the value to control the missed refresh limit in graceful restart hello messages.

ip rsvp signalling hello graceful-restart neighbor

To enable Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart capability on a neighboring router, use the **iprsvpsignallinghellograceful-restartneighbor**command in interface configuration mode. To disable graceful restart capability, use the **no** form of this command.

ip rsvp signalling hello graceful-restart neighbor *ip-address*

no ip rsvp signalling hello graceful-restart neighbor *ip-address*

Syntax Description

ip-address	IP address of a neighbor on a given interface.

Command Default

No neighboring routers have graceful restart capability enabled until you issue this command.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **iprsvpsignallinghellograceful-restartneighbor** command to enable support for graceful restart on routers helping their neighbors recover TE tunnels following stateful switchover (SSO).

Note You must issue this command on every interface of the neighboring router that you want to help restart.

Examples

The following example configures graceful restart on POS interface 1/0/0 of a neighboring router with the IP address 10.0.0.1:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface POS1/0/0
Router(config-if)# ip rsvp
 signalling hello graceful-restart neighbor 10.0.0.1
```

Related Commands

Command	Description
ip rsvp signalling hello graceful-restart mode	Enables RSVP-TE graceful restart support capability on an RP.
show ip rsvp hello graceful-restart	Displays information about RSVP-TE graceful restart hello messages.

ip rsvp signalling hello graceful-restart refresh interval

To configure the Resource Reservation Protocol (RSVP) traffic engineering (TE) refresh interval in graceful restart hello messages, use the **iprsvpsignallinghellograteful-restartrefreshinterval** command in global configuration mode. To set the interval to its default value, use the**no** form of this command.

ip rsvp signalling hello graceful-restart refresh interval *interval-value*

no ip rsvp signalling hello graceful-restart refresh interval

Syntax Description

interval-value	Frequency, in milliseconds (ms), at which a node sends hello messages to a neighbor. Valid values are from 1000 to 30000.

Command Default

1000 milliseconds (10 seconds)

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

A node periodically generates a hello message that contains a Hello Request object for all its neighbors. The frequency of those hello messages is determined by the hello interval.

Note If you change the default value for this command and you are also using the **iprsvpsignallingrefreshinterval** command, ensure that the value for the **iprsvpsignallinghellograceful-restartrefreshintervalcommandislessthanthevaluefortheiprsvpsignallingrefreshinterval** command. Otherwise, some or all of the label-switched paths (LSPs) may not be recovered after a stateful switchover (SSO) has occurred. We recommend that the value for the**iprsvpsignallingrefreshinterval**command be twice the value for the **iprsvpsignallinghellograceful-restartrefreshintervalcommand.**

Examples

In the following example, hello requests are sent to a neighbor every 5000 ms:

```
Router(config)# ip rsvp signalling hello graceful-restart refresh interval 5000
```

Related Commands

Command	Description
ip rsvp signalling hello graceful-restart dscp	Sets the DSCP value in the IP header of a RSVP TE graceful restart hello message.
ip rsvp signalling hello graceful-restart refresh misses	Sets the missed refresh limit in graceful restart hello messages.
ip rsvp signalling refresh interval	Specifies the interval between sending refresh messages for each RSVP state.

ip rsvp signalling hello graceful-restart refresh misses

To specify how many sequential Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart hello acknowledgments (ACKs) a node can miss before the node considers communication with its neighbor lost, use the **iprsvpsignallinghellograceful-restartrefreshmisses** command in global configuration mode. To return the missed refresh limit to its default value, use the **no** form of this command.

ip rsvp signalling hello graceful-restart refresh misses *msg-count*

no ip rsvp signalling hello graceful-restart refresh misses

Syntax Description

msg-count	The number of sequential hello acknowledgments (ACKs) that a node can miss before RSVP considers the state expired and tears it down. Valid values are from 4 to 10.

Command Default

The default number of sequential hello acknowledgments is 4.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T

Usage Guidelines

A hello message comprises a hello message, a Hello Request object, and a Hello ACK object. Each request is answered by an acknowledgment. If a link is congested or a router has a heavy load, set this number to a value higher than the default value to ensure that hello does not falsely declare that a neighbor is down.

Note

If you change the default value for this command and you are also using the **iprsvpsignallinghellorefreshmisses**command, ensure that the value for the **iprsvpsignallinghellograceful-restartrefreshmisses**command is less than the value for the **iprsvpsignallinghellorefreshmisses** command. Otherwise, some or all of the label-switched paths (LSPs) may not be recovered after a stateful switchover (SSO) has occurred. We recommend that the value for the**iprsvpsignallinghellorefreshmisses**command be twice the value for the **iprsvpsignallinghellograceful-restartrefreshmisses**command.

Examples

In the following example, if the node does not receive five sequential hello acknowledgments, the node declares that its neighbor is down:

```
Router(config)# ip rsvp signalling hello graceful-restart refresh misses 5
```

Related Commands

Command	Description
ip rsvp signalling hello graceful-restart dscp	Sets the DSCP value in graceful restart hello messages.
ip rsvp signalling hello graceful-restart refresh interval	Sets the refresh interval in graceful restart hello messages.
ip rsvp signalling refresh misses	Specifies the number of successive refresh messages that can be missed before RSVP removes a state from the database.
ip rsvp signalling hello refresh misses	Specifies how many Hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.

ip rsvp signalling hello graceful-restart send

To configure the time for Resource Reservation Protocol (RSVP) label switched paths (LSPs) in a Multiprotocol Label Switching (MPLS) traffic engineering (TE) network to recover or restart after a stateful switchover (SSO) occurs, use the **iprsvpsignallinghellograceful-restartsend** command in global configuration mode. To keep the default recovery and restart times, use the **no** form of this command.

ip rsvp signalling hello graceful-restart send {**recovery-time** *ms* | **restart-time** *ms*}

no ip rsvp signalling hello graceful-restart send {**recovery-time** *ms* | **restart-time** *ms*}

Syntax Description

recovery-time *ms*	Configures the time in milliseconds (ms) in outgoing hello messages to allow LSPs to recover after an SSO occurs. Values are 0 to 3600000.
restart-time *ms*	Configures the time in ms in outgoing hello messages to allow LSPs to restart after an SSO occurs. Values are 0 to 3600000.

Command Default

The default recovery and restart times of 120,000 and 30,000 ms, respecively, are in effect until you change them.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **iprsvpsignallinghellograceful-restartsend**command to give LSPs a longer time to recover or restart after an SSO occurs. Otherwise, the LSPs may not all come back up and your network performance is negatively affected.

Examples

In the following example, a recovery time of 300,000 ms is configured:

```
Router(config)# ip rsvp signalling hello graceful-restart send recovery-time 300000
```

Related Commands

Command	Description
ip rsvp signalling hello graceful-restart dscp	Sets the DSCP value in the IP header of an RSVP TE graceful restart hello message.
ip rsvp signalling hello graceful-restart mode	Enables RSVP TE graceful restart capability on an RP.
ip rsvp signalling hello graceful-restart neighbor	Enables RSVP TE graceful restart capability on a neighboring router.
ip rsvp signalling hello graceful-restart refresh interval	Configures the RSVP TE refresh interval in graceful restart hello messages.
ip rsvp signalling hello graceful-restart refresh misses	Specifies how many sequential RSVP TE graceful restart hello acknowledgments a node can miss before the node considers communication with its neighbor lost.

ip rsvp signalling hello refresh interval

To configure the Resource Reservation Protocol (RSVP) traffic engineering (TE) hello refresh interval, use the **iprsvpsignallinghellorefreshinterval** command in interface configuration mode. To set the refresh interval to its default value, use the**no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **refresh interval** *interval-value*

no ip rsvp signalling hello [**fast-reroute**] **refresh interval**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
interval-value	Frequency, in milliseconds (msec), at which a node sends hello messages to a neighbor. Valid values are from 10 to 30000 msec. **Note** Values below the default of 200 msec are not recommended, because they can cause RSVP Hellos to falsely detect a neighbor down event and unecessarily trigger Fast ReRoute.

Command Default

The default frequencyat which a node sends hello messages to a neighbor is 200 msec.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute**keyword was added.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You can configure the hello request interval on a per-interface basis. A node periodically generates a hello message containing a Hello Request object for each neighbor whose status is being tracked. The frequency of those hello messages is determined by the hello interval.

If you issue the **iprsvpsignallinghellorefreshinterval**command without the optional **fast-reroute**keyword, the command applies to Fast Reroute hellos. This command is provided for backward compatibility; however, we recommend that you use the **iprsvpsignallinghellofast-rerouterefreshinterval**command.

Examples

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh interval 5000
```

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello refresh interval 5000
```

Related Commands

Command	Description
ip rsvp signalling hello dscp	Sets the DSCP value in hello messages.
ip rsvp signalling hello graceful-restart fresh interval	Sets the refresh interval in graceful restart hello messages.
ip rsvp signalling hello reroute refresh misses	Sets the missed refresh limit in hello messages.

ip rsvp signalling hello refresh misses

To specify how many Resource Reservation Protocol (RSVP) traffic engineering (TE) hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down, use the **iprsvpsignallinghellorefreshmisses** command in interface configuration mode. To return the missed refresh limit to its default value, use the **no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **refresh misses** *msg-count*

no ip rsvp signalling hello [**fast-reroute**] **refresh misses**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
msg-count	Number of sequential hello acknowledgments that a node can miss before RSVP considers the state expired and tears it down. Valid values are from 4 to 10.

Command Default

The default number of sequential hello acknowledgments is 4.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute** keyword was added.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T

Usage Guidelines

A hello comprises a hello message, a Hello Request object, and a Hello ACK object. Each request is answered by an acknowledgment. If a link is very congested or a router has a very heavy load, set this number to a value higher than the default value to ensure that hello does not falsely declare that a neighbor is down.

If you issue the **iprsvpsignallinghellorefreshmisses**command without the optional **fast-reroute**keyword, the command applies to Fast Reroute hellos and Fast Reroute capability is enabled by default. This command is provided for backward compatibility; however, we recommend that you use the **iprsvpsignallinghellofast-rerouterefreshmisses**command.

Examples

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down and Fast Reroute is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh misses 5
```

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down and Fast Reroute is enabled by default:

```
Router(config-if)# ip rsvp signalling hello refresh misses 5
```

Related Commands

Command	Description
ip rsvp signalling hello dscp	Sets the DSCP value in hello messages.
ip rsvp signalling hello refresh interval	Sets the refresh interval in hello messages.

ip rsvp signalling hello reroute dscp

To set the differentiated services code point (DSCP) value that is in the IP header of a Resource Reservation Protocol (RSVP) traffic engineering (TE) reroute hello (for state timeout) message sent from an interface, use the **iprsvpsignallinghelloreroutedscp** command in interface configuration mode. To set the DSCP value to its default, use the **no** form of this command.

ip rsvp signalling hello reroute dscp *num*

no ip rsvp signalling hello reroute dscp

Syntax Description

num	DSCP value. Valid values are from 0 to 63.

Command Default

The default DSCP value is 48.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If a link is congested, you should set the DSCP to a value higher than 0 to reduce the likelihood that hello messages get dropped.

You configure the DSCP per interface, not per flow.

The DSCP applies to the RSVP hellos created on a specific interface. You can configure each interface independently for DSCP.

Examples

In the following example, hello messages sent from this interface have a DSCP value of 30:

```
Router(config-if)# ip rsvp signalling hello reroute dscp 30
```

Related Commands

Command	Description
ip rsvp signalling hello reroute refresh interval	Sets the hello request interval in reroute hello messages.
ip rsvp signalling hello reroute refresh misses	Sets the missed refresh limit in reroute hello messages.

ip rsvp signalling hello reroute refresh interval

To configure the Resource Reservation Protocol (RSVP) traffic engineering (TE) reroute hello (for state timeout) refresh interval, use the **iprsvpsignallinghellorerouterefreshinterval** command in interface configuration mode. To set the refresh interval to its default value, use the**no** form of this command.

ip rsvp signalling hello reroute refresh interval *interval-value*

no ip rsvp signalling hello reroute refresh interval

Syntax Description

interval-value	Frequency, in milliseconds, at which a node sends hello messages to a neighbor. Valid values are from 1000 to 30000 (1 to 30 seconds).

Command Default

The default *frequency*at which a node sends hello messages to a neighbor is 1000 milliseconds (10 seconds).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You can configure the hello request interval on a per-interface basis. A node periodically generates a hello message containing a Hello Request object for each neighbor whose status is being tracked. The frequency of those hello messages is determined by the hello interval. For some routers, if you set the interval to a value less than the default value, CPU usage may be high.

Examples

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello reroute refresh interval 5000
```

Related Commands

Command	Description
ip rsvp signalling hello reroute refresh misses	Sets the missed refresh limit in reroute hello messages.

ip rsvp signalling hello reroute refresh misses

To specify how many Resource Reservation Protocol (RSVP) traffic engineering (TE) reroute hello (for state timeout) acknowledgments (ACKs) a node can miss in a row before the node considers communication with its neighbor is down, use the **iprsvpsignallinghelloreroutrefreshmisses** command in interface configuration mode. To return the missed refresh limit to its default value, use the **no** form of this command.

ip rsvp signalling hello reroute refresh misses *msg-count*

no ip rsvp signalling hello reroute refresh misses

Syntax Description

msg-count	The number of sequential hello acknowledgments (ACKs) that a node can miss before RSVP considers the state expired and tears it down. Valid values are from 4 to 10.

Command Default

The default is 4.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

A hello comprises a hello message, a Hello Request object, and a Hello ACK object. Each request is answered by an acknowledgment. If a link is very congested or a router has a very heavy load, set this number to a value higher than the default value to ensure that hello does not falsely declare that a neighbor is down.

Examples

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down:

```
Router(config-if)# ip rsvp signalling hello reroute refresh misses 5
```

Related Commands

Command	Description
ip rsvp signalling hello reroute dscp	Sets the DSCP value in reroute hello messages.
ip rsvp signalling hello reroute refresh interval	Sets the refresh interval in reroute hello messages.

ip rsvp signalling hello statistics

To enable Hello statistics on the router, use the **iprsvpsignallinghellostatistics** command in global configuration mode. To disable Hello statistics on the router, use the **no** form of this command.

ip rsvp signalling hello statistics

no ip rsvp signalling hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

In the following example, Hello statistics are enabled on the router:

```
Router(config)# ip rsvp signalling hello statistics
```

Related Commands

Command	Description
clear ip rsvp hello instance statistics	Clears Hello statistics for an instance.

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

ip rsvp signalling initial-retransmit-delay

To configure the minimum amount of time that a Resource Reservation Protocol (RSVP)-configured router waits for an acknowledgment (ACK) message before retransmitting the same message, use the **iprsvpsignallinginitial-retransmit-delay** command in global configuration mode. To reset the delay value to its default, use the**no**form of this command.

ip rsvp signalling initial-retransmit-delay *delay-value*

no ip rsvp signalling initial-retransmit-delay

Syntax Description

delay-value	Minimum amount of time that a router waits for an ACK message before the first retransmission of the same message. The delay value ranges from 500 to 30,000 milliseconds (ms).

Command Default

The default value is 1000 ms (1.0 sec).

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the ip rsvp signalling initial-retransmit-delaycommand to configure the minimum amount of time that a router waits for an ACK message before retransmitting the same message.

If an ACK is not received for a state, the first retransmit occurs after the initial retransmit interval. If no ACK is received after the first retransmit, a second retransmit occurs. The message continues to be retransmitted, with the gap between successive retransmits being twice the previous interval, until an ACK is received. Then the message drops into normal refresh schedule if it needs to be refreshed (Path and Resv messages), or is processed (Error or Tear messages). If no ACK is received after five retransmits, the message is discarded as required.

Examples

The following command shows how to set the initial-retransmit-delay to 2 seconds:

```
Router(config)# ip rsvp signalling initial-retransmit-delay 2000
```

The following command shows how to reset the initial-retransmit-delay to the default (1.0 sec):

```
Router(config)# no ip rsvp signalling initial-retransmit-delay
```

ip rsvp signalling patherr state-removal

To reduce the amount of Resource Reservation Protocol (RSVP) traffic messages in a network, use the **iprsvpsignallingpatherrstate-removal** command in global configuration mode. To disable this function, use the **no** form of this command.

ip rsvp signalling patherr state-removal [**neighbor** *acl*]

no ip rsvp signalling patherr state-removal

Syntax Description

neighbor	(Optional) Adjacent routers that are part of a particular traffic engineering tunnel.
acl	(Optional) A simple access list with values from 1 to 99.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **iprsvpsignallingpatherrstate-removal**command to allow routers to delete Path state automatically when forwarding a PathError message, thereby eliminating the need for a subsequent PathTear message.

This command is most effective when all network nodes support this feature. All nodes need to have the latest version of Cisco IOS software configured.

This command applies only to label-switched path (LSP) flows.

Examples

The following command shows how to enable **iprsvpsignallingpatherrstate-removal**:

```
Router(config)# ip rsvp signalling patherr state-removal
```

The following command shows how to disable **iprsvpsignallingpatherrstate-removal**:

```
Router(config)# no ip rsvp signalling patherr state-removal
```

The following command shows how to enable **iprsvpsignallingpatherrstate-removal** based on an access control list (ACL):

```
Router(config)# ip rsvp signalling patherr state-removal neighbor 98
```

The following command shows how to disable **iprsvpsignallingpatherrstate-removal** based on an ACL:

```
Router(config)# no ip rsvp signalling patherr state-removal neighbor 98
```

ip rsvp signalling rate-limit

To control the transmission rate for Resource Reservation Protocol (RSVP) messages that are sent to a neighboring device during a specified amount of time, use the **ip rsvp signalling rate-limit** command in global configuration mode. To disable this function, use the **no** form of this command.

Releases Before Cisco IOS Release 12.4(20)T

ip rsvp signalling rate-limit [**burst** *number*] [**maxsize** *bytes*] [**period** *ms*]

no ip rsvp signalling rate-limit

Cisco IOS 12.0S Releases, 12.2S Releases, XE 2 Releases, Release 12.4(20)T, and Later T Releases

ip rsvp signalling rate-limit [**burst** *number*] [**limit** *number*] [**maxsize** *bytes*] [**period** *ms*]

no ip rsvp signalling rate-limit

Syntax Description

burst *number*	(Optional) Specifies the maximum number of RSVP messages that are sent to a neighboring device during each interval. Range is from 1 to 5000. Default is 8.
maxsize *bytes*	(Optional) Specifies the maximum size of the message queue, in bytes. Valid range is from 1 to 5000. Default is 2000.
period *ms*	(Optional) Specifies the length of time, in milliseconds (ms). Valid range is from 10 to 5000. Default is 20.
limit *number*	(Optional) Specifies the maximum number of messages to send per queue interval when the number of messages sent is less than the number of messages to be sent normally. Valid range is from 1 to 5000. Default is 37.

Command Default

If you do not enter this command, the default values are used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **ip rsvp msg pacing** command.
12.0(24)S	This command was modified. The **limit** keyword was added.
12.0(29)S	This command was modified. The default argument values for the **burst** and **maxsize** keywords were increased to 8 messages and 2000 bytes, respectively.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.2(3)T	This command was modified. Support for IPv6 was added.

Usage Guidelines

Use the **ip rsvp signalling rate-limit** command to prevent a burst of RSVP traffic engineering signaling messages from overflowing the input queue of a receiving device, which would cause the device to drop some messages. Dropped messages substantially delay the completion of signaling.

This command replaces the **ip rsvp msg-pacing** command.

All configurations related to the **ip rsvp signalling rate-limit** command are applicable to both IPv4 and IPv6 sessions.

Examples

The following command shows how six messages with a message queue of 500 bytes are sent every 10 ms to any neighboring device:

```
Device(config)# ip rsvp signalling rate-limit burst 6 maxsize 500 period 10
```

Related Commands

Command	Description
clear ip rsvp signalling rate-limit	Clears (sets to zero) the number of messages that were dropped because of a full queue.
debug ip rsvp rate-limit	Displays debug messages for RSVP rate-limiting events.
show ip rsvp signalling rate-limit	Displays the RSVP rate-limiting parameters.

ip rsvp signalling refresh interval

To specify the interval between sending refresh messages for each Resource Reservation Protocol (RSVP) state, use the **iprsvpsignallingrefreshinterval** command in global configuration mode. To set the interval to its default value, use the**no** form of the command.

ip rsvp signalling refresh interval *interval-value*

no ip rsvp signalling refresh interval

Syntax Description

interval-value	Time, in milliseconds, between sending refreshes for each RSVP state. The range is from 5000 to 4294967295 milliseconds; the default value is 30000.

Command Default

30000 milliseconds (30 seconds)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **iprsvpsignallingrefreshinterval** command to specify the interval between sending refresh messages for each RSVP state.

The RSVP protocol relies on a soft-state mechanism to maintain state consistency in the face of network losses. This mechanism is based on continuous refresh messages to keep a state current. Each RSVP router is responsible for sending periodic refresh messages to its neighbors.

Note If you change the default value for this command and you are also using the **iprsvpsignallinghellograceful-restartrefreshinterval** command, ensure that the value for the **iprsvpsignallinghellograceful-restartrefreshinterval** command is less than the value for the **iprsvpsignallingrefreshinterval** command. Otherwise, some or all of the label-switched paths (LSPs) may not be recovered after a stateful switchover (SSO) has occurred. We recommend that the value for the **iprsvpsignallingrefreshinterval** command be twice the value for the **iprsvpsignallinghellograceful-restartrefreshinterval** command.

Examples

The following example shows how to specify a refresh interval of 60000 milliseconds (60 seconds):

```
Router(config)# ip rsvp signalling refresh interval 60000
```

The following example returns the refresh interval to the default value of 30 seconds:

```
Router(config)# no ip rsvp signalling refresh interval
```

Related Commands

Command	Description
ip rsvp signalling refresh misses	Specifies the number of successive refresh messages that can be missed before RSVP removes a state from the database.

ip rsvp signalling refresh misses

To specify the number of successive refresh messages that can be missed before Resource Reservation Protocol (RSVP) removes a state from the database, use the **iprsvpsignallingrefreshmisses** command in global configuration mode. To return the missed refresh limit to its default value, use the **no** form of this command.

ip rsvp signalling refresh misses *msg-count*

no ip rsvp signalling refresh misses

Syntax Description

msg-count	Number of successive refresh messages that can be missed before RSVP considers the state expired and tears it down. The range is 2 to 10. The default is 4.

Command Default

4 messages

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the**iprsvpsignallingrefreshmisses**command to specify the number of successive refresh messages that can be missed before RSVP regards the router state as expired and removes that state from the database.

Note

If you change the default value for this command and you are also using the **iprsvpsignallinghellograceful-restartrefreshmisses**command, ensure that the value for the **iprsvpsignallinghellograceful-restartrefreshmisses** command is less than the value for the **iprsvpsignallingrefreshmisses**command. Otherwise, some or all of the label-switched paths (LSPs) may not be recovered after a stateful switchover (SSO) has occurred. We recommend that the value for the **iprsvpsignallingrefreshmisses**command be twice the value for the **iprsvpsignallinghellograceful-restartrefreshmisses**command.

Examples

The following example shows how to specify a missed refresh limit of 6 messages:

```
Router(config)# ip rsvp signalling refresh misses 6
```

The following example shows how to return the refresh misses limit to the default value of 4:

```
Router(config)# no ip rsvp signalling refresh misses
```

Related Commands

Command	Description
ip rsvp signalling refresh interval	Specifies the interval between sending refresh messages for each RSVP state.

ip rsvp signalling refresh reduction

To enable Resource Reservation Protocol (RSVP) refresh reduction, use the**iprsvpsignallingrefreshreduction** command in global configuration mode. To disable refresh reduction, use the **no** form of this command.

ip rsvp signalling refresh reduction

no ip rsvp signalling refresh reduction

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

RSVP refresh reduction is a set of extensions to reduce the messaging load imposed by RSVP and to help it scale to support larger numbers of flows.

The following features of the refresh reduction standard (RFC 2961) are supported and will be turned on with this command:

- Setting the refresh-reduction-capable bit in message headers
- Message-Identifier (ID) usage
- Reliable messaging with rapid retransmit, acknowledgement (ACK) messages, and MESSAGE_ID objects
- Summary refresh extension
- Bundle messages (reception only)

Refresh reduction requires the cooperation of the neighbor to operate; for this purpose, the neighbor must also support the standard. If the router detects that a directly connected neighbor is not supporting the refresh reduction standard (either through observing the refresh-reduction-capable bit in messages received from the next hop, or by sending a MESSAGE_ID object to the next hop and receiving an error), refresh reduction will not be used on this link irrespective of this command.

Examples

The following command shows how to enable RSVP refresh reduction:

```
Router(config)# ip rsvp signalling refresh reduction
```

The following command shows how to disable RSVP refresh reduction:

```
Router(config)# no ip rsvp signalling refresh reduction
```

Related Commands

Command	Description
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp signalling refresh reduction	Displays refresh-reduction parameters for RSVP messages.

ip rsvp signalling refresh reduction ack-delay

To configure the maximum amount of time that a Resource Reservation Protocol (RSVP)-configured router holds on to an acknowledgment (ACK) message before sending it, use the**iprsvpsignallingrefreshreductionack-delay**command in global configuration mode. To reset the ack-delay value to its default, use the **no**form of this command.

ip rsvp signalling refresh reduction ack-delay *delay-value*

no ip rsvp signalling refresh reduction ack-delay

Syntax Description

delay-value	Maximum amount of time that a router holds on to an ACK message before sending it. Values range from 100 to 10000 milliseconds (ms).

Command Default

The default value is 250 ms (0.25 sec).

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **iprsvpsignallingrefreshreductionack-delay**command to configure the maximum amount of time that an RSVP-configured router keeps an ACK message before sending it.

Examples

The following command shows how to set the ack-delay value to 1 second:

```
Router(config)# ip rsvp signalling refresh reduction ack-delay 1000
```

The following command shows how to set the ack-delay value to the default value:

```
Router(config)# no ip rsvp signalling refresh reduction ack-delay
```

ip rsvp snooping

To enable Resource Reservation Protocol (RSVP) snooping in a specific set of VLANs, use the **ip rsvp snooping** command in global configuration mode. To disable RSVP snooping, use the **no** form of this command.

ip rsvp snooping [**vlan** *vlan-id* | **vlan-range** *vlan-id-start vlan-id-end*]

no ip rsvp snooping [**vlan** *vlan-id* | **vlan-range** *vlan-id-start vlan-id-end*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies the VLAN in which RSVP snooping must be enabled.
vlan-range *vlan-id-start vlan-id-end*	(Optional) Specifies a range of VLANs in which RSVP snooping must be enabled.

Command Default

RSVP snooping is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(44)SE	This command was introduced.

Usage Guidelines

Use the **ip rsvp snooping** command to enable or disable RSVP snooping in a specific VLAN or range of VLANs. Specifying VLANs is optional. The keyword argument pairs **vlan** *vlan-id* and **vlan-range** *vlan-id-start vlan-id-end* are visible only on platforms that support per-VLAN snooping. If you do not specify VLAN details, snooping is enabled on all VLANs. Using this command more than once will not disable the previous configurations. In the event of creating a new VLAN, if RSVP snooping is enabled on all VLANs, RSVP snooping will be enabled on the new VLAN too. If you use the **no ip rsvp snooping** command without specifying any VLANs, RSVP snooping will be disabled in all VLANs.

Examples

The following example shows how to enable RSVP snooping in a specific VLAN:

```
Device> enable
Device# configure terminal
Device(config)# ip rsvp snooping vlan 10
```

Related Commands

Command	Description
show ip rsvp snooping	Displays the list of VLANs in which RSVP snooping is enabled.

ip rsvp source

To configure a Resource Reservation Protocol (RSVP) router to populate an address other than the native interface address in the previous hop (PHOP) address field of the PHOP object when forwarding a PATH message onto that interface, use the **iprsvpsource** command in interface configuration mode. To keep the native interface address in the PHOP address field, use the **no** form of this command.

ip rsvp source {**address** *ip-address* | **interface** *type number*}

no ip rsvp source

Syntax Description

address *ip-address*	IP address for the PHOP address field.
interface *type number*	Interface type and number that is used as the source for the PHOP address field.

Command Default

The native interface address is written in the PHOP address field.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Examples

The following example configures IP address 10.1.3.13 for the PHOP address field:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ethernet 0/0
Router(config-if)# ip rsvp bandwidth
Router(config-if)# ip rsvp source address 10.1.3.13
Router(config-if)# end
```

The following example configures loopback interface 0 as the interface whose address is used in the PHOP address field:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ethernet 1/0
Router(config-if)# ip rsvp bandwidth
Router(config-if)# ip rsvp source interface loopback 0
Router(config-if)# end
```

Related Commands

Command	Description
show ip rsvp interface	Displays RSVP-related information.

ip rsvp svc-required

To enable creation of a switched virtual circuit (SVC) to service any new Resource Reservation Protocol (RSVP) reservation made on the interface or subinterface of an Enhanced ATM port adapter (PA-A3), use the **iprsvpsvc-required** command in interface configuration mode. To disable SVC creation for RSVP reservations, use the **no** form of this command.

ip rsvp svc-required

no ip rsvp svc-required

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies exclusively to the RSVP-ATM QoS Interworking feature.

Usually reservations are serviced when RSVP classifies packets and a queueing mechanism schedules them for transmission to manage congestion. Traditionally, RSVP is used with weighted fair queueing (WFQ). When RSVP is coupled with WFQ, all of the packets visible to WFQ are also visible to RSVP, which allows RSVP to identify and take action on packets important to it. In this case, WFQ provides bandwidth guarantees.

However, when the **iprsvpsvc-required** command is used to configure an interface or subinterface, a new SVC is established and used to service each new reservation on the interface. ATM SVCs are used to provide bandwidth guarantees and NetFlow is used on input interfaces to make data packets visible to RSVP.

Note When RSVP is enabled, all packets are processed by the Route Switch Processor (RSP).

This command must be executed on both ends of an SVC driven by RSVP. This command is supported only for the Enhanced ATM port adapter (PA-A3) and its subinterfaces.

Note For this command to take effect, NetFlow must be enabled. Therefore, the **iproute-cacheflow** command must precede this command in the configuration.

Use the **showiprsvpinterface** command to determine whether this command is in effect for any interface or subinterface.

Examples

The following example signals RSVP that reservations made on ATM interface 2/0/0 will be serviced by creation of an SVC:

```
interface atm2/0/0
 ip rsvp svc-required
```

Related Commands

Command	Description
ip route-cache flow	Enables NetFlow switching for IP routing.
ip rsvp atm-peak-rate-limit	Sets a limit on the peak cell rate of reservations for all newly created RSVP SVCs established on the current interface or any of its subinterfaces.
ip rsvp precedence	Allows you to set the IP Precedence values to be applied to packets that either conform to or exceed the RSVP flowspec.
show ip rsvp interface	Displays RSVP-related interface information.

ip rsvp tos

To enable the router to mark the five low-order type of service (ToS) bits of the IP header ToS byte for packets in a Resource Reservation Protocol (RSVP) reserved path using the specified values for traffic that either conforms to or exceeds the RSVP flowspec, use the **iprsvptos** command in interface configuration mode. To remove existing settings for the ToS bits, use the **no** form of this command; if neither the **conform**nor **exceed** keyword is specified, all settings for the ToS bits are removed.

ip rsvp tos conform *tos-value* **exceed** *tos-value*

no ip rsvp tos [**conform**] [**exceed**]

Syntax Description

conform *tos-value*	Specifies a ToS value in the range from 0 to 31 for traffic that conforms to the RSVP flowspec. The ToS value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified. When used with the **no** form of the command, the **conform** keyword is optional.
exceed *tos-value*	(Optional) Specifies a ToS value in the range from 0 to 31 for traffic that exceeds the RSVP flowspec. The ToS byte value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified. When used with the **no** form of the command, the **exceed** keyword is optional.

Command Default

The ToS bits of the ToS byte are left unmodified when this command is not used. (The default behavior is equivalent to use of the **noiprsvptos** command.)

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Packets in an RSVP reserved path are divided into two classes: those that conform to the reservation flowspec and those that correspond to a reservation but that exceed, or are outside, the reservation flowspec.

The **iprsvptos** command allows you to set the ToS values to be applied to packets belonging to these two classes. You must specify the ToS value for at least one class of traffic when you use this command. You can use a single instance of the command to specify values for both classes, in which case you can specify the **conform** and **exceed** keywords in either order.

As part of its input processing, RSVP uses the **iprsvptos** command configuration to set the ToS bits of the ToS byte on conforming and nonconforming packets. If per-virtual circuit (VC) VIP-distributed Weighted Random Early Detection (DWRED) is configured, the system uses the ToS bit and IP Precedence bit settings on the output interface in its packet drop process. The ToS bit and IP Precedence bit settings of a packet can also be used by interfaces on downstream routers.

Execution of the **iprsvptos** command causes ToS bit values for all preexisting reservations on the interface to be modified.

Note RSVP must be enabled on an interface before you can use this command; that is, use of the **iprsvpbandwidth** command must precede use of the **iprsvptos** command. RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Note The **iprsvptos** command sets bits 0 to 4 so that in combination with the IP Precedence bit settings every bit in the ToS byte is set. Use of these bits is made with full knowledge of the fact that certain canonical texts that address the ToS byte specify that only bits 1 to 4 are used as the ToS bits.

RSVP receives packets from the underlying forwarding mechanism. Therefore, to use the **iprsvptos** command to set the ToS bits, one of the following features is required:

- Weighted fair queueing (WFQ) must be enabled on the interface.
- RSVP switched virtual circuits (SVCs) must be used.
- NetFlow must be configured to assist RSVP.

Note Use of the **no** form of this command is not equivalent to giving the**iprsvptos0**command, which sets all precedence on the packets to 0, regardless of previous precedence setting.

Examples

The following example sets the ToS bits value to 4 for all traffic on ATM interface 1 that conforms to the RSVP flowspec. ToS bits on packets exceeding the flowspec are not altered.

```
interface atm1
 ip rsvp tos conform 4
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp flow-assist	Enables RSVP to attach itself to NetFlow so that it can leverage NetFlow services.
ip rsvp policy cops minimal	Lowers the COPS server's load and improves latency times for messages on the governed router.
show ip rsvp	Displays the IP Precedence and ToS bit values to be applied to packets that either conform to or exceed the RSVP flowspec for a given interface.

ip rsvp transport

To create a Resource Reservation Protocol (RSVP) transport session, use the **iprsvptransport** command in global configuration mode. To disable the RSVP transport session, use the **no** form of this command.

ip rsvp transport {**client** *client-id* | **statistics**}

no ip rsvp transport {**client** *client-id* | **statistics**}

Syntax Description

client	Initiates RSVP transport client.
client-id	Client identifier. The range is from 1 to 65535.
statistics	Configures RSVP transport protocol (TP) information buffer size.

Command Default

RSVP is configured as transport protocol.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

You can use the **iprsvptransport** command to configure RSVP to be used as transport mechanism for the clients. The *client-id* is used for identification of the client that initiates the RSVP as a transport protocol. The **statistics** keyword is used to record statistics for RSVP TP sessions. The statistics recorded includes information passed by RSVP to the RSVP TP client as part of callback. The maximum amount of information that can be recorded is 32 MB.

The **iprsvptransport** command enables a router to simulate a host generating RSVP PATH message. This command is used for testing and debugging purposes.

Examples

The following example shows how to identify a client to establish an RSVP transport session:

```
Router> enable
```

```
Router# configure terminal
Router(config)# ip rsvp transport client 12
```

Related Commands

Command	Description
ip rsvp transport sender-host	Registers a transport client ID with RSVP.

ip rsvp transport sender-host

To register a transport client ID with Resource Reservation Protocol (RSVP), use the **iprsvptransportsender-host** command in global configuration mode. To disable the static RSVP host path configuration, use the **no** form of this command.

ip rsvp transport sender-host [**tcp** | **udp**] *destination-address source-address ip-protocol dest-port source-port client-id init-id instance-id* [**vrf** *vrf-name*] [**data** *data-value*]

no ip rsvp transport sender-host [**tcp** | **udp**] *destination-address source-address ip-protocol dest-port source-port client-id init-id instance-id* [**vrf** *vrf-name*] [**data** *data-value*]

Syntax Description

tcp	(Optional) Specifies TCP to be used as transport mechanism.
udp	(Optional) Specifies User Datagram Protocol (UDP) to be used as transport mechanism.
destination-address	Destination address to where the PATH message is sent.
source-address	Source address from where the PATH message is sent.
ip-protocol	Identifier for configuring RSVP as a transport protocol. The range is from 0 to 255.
dest-port	Destination port to which the PATH message is sent.
source-port	Source port from which the PATH message is sent.
client-id	Identifier that initiates RSVP client.
init-id	Hostname or IP address that identifies the node initiating the transport service request.
instance-id	Instance ID that identifies the transport service request from a particular client application and from a particular initiator. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Configures VPN Routing and Forwarding (VRF) instance on the RSVP client.
data *data-value*	(Optional) Configures the RSVP transport data value.

Command Default

The static RSVP host path is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Use the **iprsvptransportsender-host** command to configure the RSVP transport proxy path. When this command is configured, RSVP sends PATH messages downstream.

Examples

The following example shows how to configure an RSVP sender host path:

```
Router> enable
Router# configure terminal
Router(config)# ip rsvp transport sender-host 10.1.1.1 10.2.1.1 2 3 4 3 192.168.1.2 2 vrf
vrf1 data d1
```

Related Commands

Command	Description
ip rsvp transport	Configures RSVP as transport protocol.

ip rsvp tunnel overhead-percent

To manually override the Resource Reservation Protocol (RSVP) percentage bandwidth, use the **iprsvptunneloverhead-percent**command in interface configuration mode. To restore the tunnel overhead percentage to its default values, use the **no** form of this command.

ip rsvp tunnel overhead-percent *percentage*

no ip rsvp tunnel overhead-percent

Syntax Description

percentage	Percentage overhead on the tunnel.

Command Default

The percentage overhead for generic routing encapsulation (GRE) or multipoint generic routing encapsulation (mGRE) interfaces is 4 percent. The percentage overhead for GRE and mGRE with IPsec interfaces ranges from 4 to 15 percent, with an average of 10 percent.

Command Modes

Interface configuration mode (config-if)

Command History

Release	Modification
15.1(2)T	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

During the bandwidth admission control, the Cisco IOS software must consider the additional IP overhead introduced because of tunneling and a possible encryption over these tunnels. The default values for the overhead depends on the average size of an Internet packet. However, you can manually override the default values by using the **iprsvptunneloverhead-percent**command.

For example, when the Cisco IOS software gets a reservation request for 100 bytes, and if the outbound interface is a GRE or an mGRE interface, then a bandwidth reservation request for 104 bytes is made available locally on that tunnel interface. In case the GRE or mGRE interface is in protected mode, 110 bytes is requested on the respective link. This IP overhead does not affect the bandwidth signaled via RSVP.

Examples

The following example shows how to configure the router to manually override the percentage bandwidth:

```
Router(config)# interface tunnel 1
Router(config-if)# ip rsvp tunnel overhead-percent 20
```

Related Commands

Command	Description
show ip rsvp interface detail	Displays the hello configuration for all interfaces.

ip rsvp udp-multicasts

To instruct the router to generate User Datagram Protocol (UDP)-encapsulated Resource Reservation Protocol (RSVP) multicasts whenever it generates an IP-encapsulated multicast packet, use the **iprsvpudp-multicasts**command in interface configuration mode. To disable this function, use the **no** form of this command.

ip rsvp udp-multicasts [*multicast-address*]

no ip rsvp udp-multicasts [*multicast-address*]

Syntax Description

multicast-address	(Optional) Host name or UDP multicast address of router.

Command Default

The generation of UDP multicasts is disabled. If a system sends a UDP-encapsulated RSVP message to the router, the router begins using UDP for contact with the neighboring system. The router uses multicast address 224.0.0.14 and starts sending to UDP port 1699. If the command is entered with no specifying multicast address, the router uses the same multicast address.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to instruct a router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet. Some hosts require this trigger from the router.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example reserves up to 7500 kbps on Ethernet interface 2, with up to 1 Mbps per flow. The router is configured to use UDP encapsulation with the multicast address 224.0.0.14.

```
interface ethernet 2
 ip rsvp bandwidth 7500 1000
 ip rsvp udp-multicasts 224.0.0.14
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving and forwarding RSVP PATH messages.

ip rsvp udp neighbor

To enable neighbor routers to process and send Resource Reservation Protocol (RSVP) control packets over UDP, use the **ip rsvp udp neighbor** command in global configuration mode. To disable neighbor routers to process and send RSVP control packets over UDP, use the **no** form of the command.

ip rsvp udp neighbor *neighbor-IP-address* **router** [**vrf** *vrf-name*]

no ip rsvp udp neighbor *neighbor-IP-address* **router** [**vrf** *vrf-name*]

Syntax Description

neighbor-IP-address	IP address of the neighbor router.
router	Specifies that the neighbor is a router.
vrf *vrf-name*	(Optional). Specifies the Virtual Routing and Forwarding (VRF) instance name.

Command Default

The **ip rsvp udp neighbor** command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

The **ip rsvp udp neighbor** command can be used to enable a neighbor router to communicate to the first hop router over UDP and not raw IP. Also, this command can be used in a scenario where a firewall that is located in between two routers drops raw IP packets due to security concerns, but allows UDP packets.

Examples

The following example shows how to enable a neighbor router with IP address 10.1.1.1 to process and send RSVP control packets over UDP:

```
Device> enable
Device# configure terminal
Device(config)# ip rsvp udp neighbor 10.1.1.1 router vrf vrf-1
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for an IP on an interface.

ip rtp compression-connections

To specify the total number of Real-Time Transport Protocol (RTP) header compression connections that can exist on an interface, use the **iprtpcompression-connections**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip rtp compression-connections *number*

no ip rtp compression-connections

Syntax Description

number	Number of RTP header compression connections the cache supports, in the range from 3 to 1000.

Command Default

For PPP and High-Level Data Link Control (HDLC) interfaces, the default is 16 compression connections.

For Frame Relay interfaces, the default is 256 compression connections.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(7)T	For PPP and HDLC interfaces, the maximum number of compression connections increased from 256 to 1000. For Frame Relay interfaces, the maximum number of compression connections increased from 32 to 256. The default number of compression connections was increased from 32 (fixed) to 256 (configurable).
12.1(4)E	This command was implemented on the Cisco 7100 series.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You should configure one connection for each RTP call through the specified interface.

Each connection sets up a compression cache entry, so you are in effect specifying the maximum number of cache entries and the size of the cache. Too few cache entries for the specified interface can lead to degraded performance, and too many cache entries can lead to wasted memory.

Note Both ends of the serial connection must use the same number of cache entries.

Examples

The following example changes the number of RTP header compression connections supported to 150:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression
Router(config-if)# ip rtp compression-connections 150
Router(config-if)# end
```

Related Commands

Command	Description
ip rtp header-compression	Enables RTP header compression.
show ip rtp header-compression	Displays RTP header compression statistics.

ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression, use the **iprtpheader-compression**command in interface configuration mode. To disable RTP header compression, use the **no** form of this command.

ip rtp header-compression [**passive** | **iphc-format** | **ietf-format**] [**periodic-refresh**]

no ip rtp header-compression [**passive** | **iphc-format** | **ietf-format**] [**periodic-refresh**]

Syntax Description

passive	(Optional) Compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed. If you do not specify the **passive** keyword, all RTP packets are compressed.
iphc-format	(Optional) Indicates that the IP Header Compression (IPHC) format of header compression will be used.
ietf-format	(Optional) Indicates that the Internet Engineering Task Force (IETF) format of header compression will be used.
periodic-refresh	(Optional) Indicates that the compressed IP header will be refreshed periodically.

Command Default

Disabled

For PPP interfaces, the default format for header compression is the IPHC format.

For High-Level Data Link Control (HDLC) and Frame Relay interfaces, the default format for header compression is the original proprietary Cisco format. The maximum number of compression connections for the proprietary Cisco format is 256.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0	This command was integrated into Cisco IOS Release 12.0. This command was modified to include the **iphc-format** keyword.

Release	Modification
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T. This command was modified to include the **periodic-refresh** keyword.
12.3(4)T	This command was modified to include the **ietf-format** keyword.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Compressing Headers

You can compress IP/User Datagram Protocol (UDP)/RTP headers to reduce the size of your packets. Compressing headers is especially useful for RTP because RTP payload size can be as small as 20 bytes, and the uncompressed header is 40 bytes.

The passive Keyword

By default, the **iprtpheader-compression** command compresses outgoing RTP traffic. If you specify the **passive** keyword, outgoing RTP traffic is compressed only if *incoming* RTP traffic on the *same* interface is compressed. If you do not specify the **passive** keyword, *all* outgoing RTP traffic is compressed.

The **passive** keyword is ignored on PPP interfaces. PPP interfaces negotiate the use of header-compression, regardless of whether the **passive** keyword is specified. Therefore, on PPP interfaces, the **passive** keyword is replaced by the IPHC format, the default format for PPP interfaces.

The iphc-format Keyword

The **iphc-format** keyword indicates that the IPHC format of header compression that will be used. For PPP and HDLC interfaces, when the **iphc-format** keyword is specified, TCP header compression is also enabled. For this reason, the **iptcpheader-compression** command appears in the output of the **showrunning-config** command. Since both RTP header compression and TCP header compression are enabled, both UDP packets and TCP packets are compressed.

The **iphc-format** keyword includes checking whether the destination port number is even and is in the ranges of 16,385 to 32,767 (for Cisco audio) or 49,152 to 65,535 (for Cisco video). Valid RTP packets that meet the criteria (that is, the port number is even and is within the specified range) are compressed using the compressed RTP packet format. Otherwise, packets are compressed using the less-efficient compressed non-TCP packet format.

The **iphc-format** keyword is not available for interfaces that use Frame Relay encapsulation.

Note The header compression format (in this case, IPHC) must be the same at *both* ends of the network. That is, if you specify the **iphc-format** keyword on the local router, you must also specify the **iphc-format** keyword on the remote router.

The ietf-format Keyword

The **ietf-format**keyword indicates that the IETF format of header compression will be used. For HDLC interfaces, the**ietf-format**keyword compresses only UDP packets. For PPP interfaces, when the **ietf-format** keyword is specified, TCP header compression is also enabled. For this reason, the **iptcpheader-compression** command appears in the output of the **showrunning-config** command. Since both RTP header compression and TCP header compression are enabled, both UDP packets and TCP packets are compressed.

With the **ietf-format** keyword, any even destination port number higher than 1024 can be used. Valid RTP packets that meet the criteria (that is, the port number is even and is higher than 1024) are compressed using the compressed RTP packet format. Otherwise, packets are compressed using the less-efficient compressed non-TCP packet format.

The **ietf-format** keyword is not available for interfaces that use Frame Relay encapsulation.

Note The header compression format (in this case, IETF) must be the same at *both* ends of the network. That is, if you specify the **ietf-format**keyword on the local router, you must also specify the **ietf-format** keyword on the remote router.

Support for Serial Lines

RTP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection.

Unicast or Multicast RTP Packets

This command can compress unicast or multicast RTP packets, and, hence, multicast backbone (MBONE) traffic can also be compressed over slow links. The compression scheme is beneficial only when you have small payload sizes, as in audio traffic.

Custom or Priority Queueing

When you use the**iprtpheader-compression** command and configure custom or priority queueing on an encapsulated HDLC or Frame Relay interface, the compressed packets may go to the default queue instead of the user-defined queue, which results in protocol flaps (loss of keepalives). Therefore, we recommend that you use the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) model for configuring QoS features.

Examples

The following example enables RTP header compression on the Serial1/0 interface and limits the number of RTP header compression connections to 10. In this example, the optional **iphc-format** keyword of the**iprtpheader-compression**command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# end
```

The following example enables RTP header compression on the Serial2/0 interface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the**iprtpheader-compression**command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression ietf-format
Router(config-if)# ip rtp compression-connections 20
Router(config-if)# end
```

In the following example, RTP header compression is enabled on the Serial1/0 interface and the optional **periodic-refresh** keyword of the**iprtpheader-compression**command is specified:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format periodic-refresh
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# end
```

Related Commands

Command	Description
clear ip rtp header-compression	Clears RTP header compression structures and statistics.
ip rtp compression-connections	Specifies the total number of RTP header compression connections that can exist on an interface.
show ip rtp header-compression	Displays RTP header compression statistics.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

ip rtp priority

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **iprtppriority**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **iprtppriority**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To reserve a strict priority queue for a set of Real-Time Transport Protocol (RTP) packet flows belonging to a range of User Datagram Protocol (UDP) destination ports, use the **iprtppriority** command in interface configuration mode. To disable the strict priority queue, use the **no** form of this command.

ip rtp priority *starting-rtp-port-number port-number-range bandwidth*

no ip rtp priority

Syntax Description

starting-rtp-port-number	The starting RTP port number. The lowest port number to which the packets are sent. The port number can be a number from 2000 to 65,535.
port-number-range	The range of UDP destination ports. Number, when added to the *starting-rtp-port-number*argument, that yields the highest UDP port number. The range of UDP destination ports is from 0 to 16,383.
bandwidth	Maximum allowed bandwidth, in kbps. The maximum allowed bandwidth is from 0 to 2000.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

This command is most useful for voice applications, or other applications that are delay-sensitive.

This command extends and improves on the functionality offered by the **iprtpreserve** command by allowing you to specify a range of UDP/RTP ports whose voice traffic is guaranteed strict priority service over any other queues or classes using the same output interface. Strict priority means that if packets exist in the priority queue, they are dequeued and sent first--that is, before packets in other queues are dequeued. We recommend that you use the **iprtppriority** command instead of the **iprtpreserve** command for voice configurations.

This command can be used in conjunction with either weighted fair queueing (WFQ) or class-based WFQ (CBWFQ) on the same outgoing interface. In either case, traffic matching the range of ports specified for the priority queue is guaranteed strict priority over other CBWFQ classes or WFQ flows; voice packets in the priority queue are always serviced first.

Remember the following guidelines when using the **iprtppriority** command:

- When used in conjunction with WFQ, the **iprtppriority** command provides strict priority to voice, and WFQ scheduling is applied to the remaining queues.
- When used in conjunction with CBWFQ, the **iprtppriority** command provides strict priority to voice. CBWFQ can be used to set up classes for other types of traffic (such as Systems Network Architecture [SNA]) that need dedicated bandwidth and need to be treated better than best effort and not as strict priority; the nonvoice traffic is serviced fairly based on the weights assigned to the enqueued packets. CBWFQ can also support flow-based WFQ within the default CBWFQ class if so configured.

Remember the following guidelines when configuring the *bandwidth* argument:

- It is always safest to allocate to the priority queue slightly more than the known required amount of bandwidth, to allow room for network bursts.
- The IP RTP Priority admission control policy takes RTP header compression into account. Therefore, while configuring the *bandwidth* argument of the **iprtppriority** command you need to configure only

for the bandwidth of the compressed call. Because the *bandwidth* argument is the maximum total bandwidth, you need to allocate enough bandwidth for all calls if there will be more than one call.

- Configure a bandwidth that allows room for Layer 2 headers. The bandwidth allocation takes into account the payload plus the IP, UDP, and RTP headers but does not account for Layer 2 headers. Allowing 25 percent bandwidth for other overhead is conservative and safe.
- The sum of all bandwidth allocation for voice and data flows on an interface cannot exceed 75 percent of the total available bandwidth, unless you change the default maximum reservable bandwidth. To change the maximum reservable bandwidth, use the **max-reserved-bandwidth** command on the interface.

For more information on IP RTP Priority bandwidth allocation, refer to the section “IP RTP Priority” in the chapter “Congestion Management Overview” in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example first defines a CBWFQ configuration and then reserves a strict priority queue with the following values: a starting RTP port number of 16384, a range of 16383 UDP ports, and a maximum bandwidth of 40 kbps:

```
! The following commands define a class map:
class-map class1
 match access-group 101
 exit
! The following commands create and attach a policy map:
policy-map policy1
class class1
 bandwidth 3000
 queue-limit 30
 random-detect
 random-detect precedence 0 32 256 100
 exit
interface Serial1
 service-policy output policy1
! The following command reserves a strict priority queue:
 ip rtp priority 16384 16383 40
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
fair queue (WFQ)	Enables WFQ for an interface.
frame-relay ip rtp priority	Reserves a strict priority queue on a Frame Relay PVC for a set of RTP packet flows belonging to a range of UDP destination ports.
ip rtp reserve	Reserves a special queue for a set of RTP packet flows belonging to a range of UDP destination ports.
max-reserved-bandwidth	Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority.

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
ppp multilink	Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation.
ppp multilink fragment-delay	Configures a maximum delay allowed for transmission of a packet fragment on an MLP bundle.
ppp multilink interleave	Enables interleaving of RTP packets among the fragments of larger packets on an MLP bundle.
priority	Gives priority to a class of traffic belonging to a policy map.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.

ip tcp compression-connections

To specify the total number of Transmission Control Protocol (TCP) header compression connections that can exist on an interface, use the **ip tcp compression-connections** command in interface configuration mode.To restore the default, use the **no**form of this command.

ip tcp compression-connections *number*

no ip tcp compression-connections

Syntax Description

number	Number of TCP header compression connections the cache supports, in the range from 3 to 256.

Command Default

For PPP and High-Level Data Link Control (HDLC) interfaces, the default is 16 compression connections.

For Frame Relay interfaces, the default is 256 compression connections.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	For Frame Relay interfaces, the maximum number of compression connections increased from 32 to 256. The default number of compression connections was increased from 32 (fixed) to 256 (configurable).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You should configure one connection for each TCP connection through the specified interface.

Each connection sets up a compression cache entry, so you are in effect specifying the maximum number of cache entries and the size of the cache. Too few cache entries for the specified interface can lead to degraded performance, and too many cache entries can lead to wasted memory.

Note Both ends of the serial connection must use the same number of cache entries.

Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

Related Commands

Command	Description
ip tcp header-compression	Enables TCP header compression.
show ip tcp header-compressions	Displays TCP header compression statistics.

ip tcp header-compression

To enable Transmission Control Protocol (TCP) header compression, use the **ip tcp header-compression** command in interface configuration mode.To disable compression, use the **no**form of this command.

ip tcp header-compression [**passive** | **iphc-format** | **ietf-format**]

no ip tcp header-compression [**passive** | **iphc-format** | **ietf-format**]

Syntax Description

passive	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the **passive** keyword, all TCP packets are compressed.
iphc-format	(Optional) Indicates that the IP Header Compression (IPHC) format of header compression will be used.
ietf-format	(Optional) Indicates that the Internet Engineering Task Force (IETF) format of header compression will be used.

Command Default

For PPP interfaces, the default format for header compression is the IPHC format.

For High-Level Data Link Control (HDLC) and Frame Relay interfaces, the default format is as described in RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links.*

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0	This command was integrated into Cisco IOS Release 12.0. This command was modified to include the **iphc-format** keyword.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. This command was modified to include the **ietf-format** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection. Compressing the TCP header can speed up Telnet connections dramatically.

In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets and file transfers use large packets. This feature only compresses the TCP header, so it has no effect on User Datagram Protocol (UDP) packets or other protocol headers.

The passive Keyword

By default, the **ip tcp header-compression** command compresses outgoing TCP traffic. If you specify the **passive** keyword, outgoing TCP traffic is compressed only if incoming TCP traffic on the same interface is compressed. If you do not specify the **passive** keyword, all outgoing TCP traffic is compressed.

For PPP interfaces, the **passive** keyword is ignored. PPP interfaces negotiate the use of header-compression, regardless of whether the **passive** keyword is specified. Therefore, on PPP interfaces, the **passive** keyword is replaced by the IPHC format, the default format for PPP interfaces.

The iphc-format Keyword

The **iphc-format** keyword indicates that the IPHC format of header compression will be used. For PPP and HDLC interfaces, when the **iphc-format** keyword is specified, Real-Time Transport Protocol (RTP) header compression is also enabled. For this reason, the **ip rtp header-compression** command appears in the output of the **show running-config** command. Since both TCP header compression and RTP header compression are enabled, both TCP packets and UDP packets are compressed.

The **iphc-format** keyword is not available for interfaces that use Frame Relay encapsulation.

Note The header compression format (in this case, IPHC) must be the same at *both* ends of the network. That is, if you specify the **iphc-format** keyword on the local router, you must also specify the **iphc-format** keyword on the remote router.

The ietf-format Keyword

The **ietf-format** keyword indicates that the IETF format of header compression will be used. For HDLC interfaces, the **ietf-format** keyword compresses only TCP packets. For PPP interfaces, when the **ietf-format** keyword is specified, RTP header compression is also enabled. For this reason, the **ip rtp header-compression** command appears in the output of the **show running-config** command. Since both TCP header compression and RTP header compression are enabled, both TCP packets and UDP packets are compressed.

The **ietf-format** keyword is not available for interfaces that use Frame Relay encapsulation.

Note The header compression format (in this case, IETF) must be the same at *both* ends of the network. That is, if you specify the **ietf-format**keyword on the local router, you must also specify the **ietf-format** keyword on the remote router.

Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

The following example enables RTP header compression on the Serial1/0.0 subinterface and limits the number of RTP header compression connections to 10. In this example, the optional **iphc-format** keyword of the **ip tcp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression iphc-format
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

The following example enables RTP header compression on the Serial2/0.0 subinterface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the **ip tcp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression ietf-format
Router(config-if)# ip tcp compression-connections 20
Router(config-if)# end
```

Related Commands

Command	Description
ip tcp compression-connections	Specifies the total number of TCP header compression connections that can exist on an interface.
show ip tcp header-compression	Displays TCP/IP header compression statistics.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

iphc-profile

To create an IP Header Compression (IPHC) profile and to enter IPHC-profile configuration mode, use the **iphc-profile** command in global configuration mode. To attach an existing IPHC profile to an interface or subinterface, use the **iphc-profile** command in interface configuration mode. To delete the IPHC profile, use the **no** form of this command.

iphc-profile *profile-name* {**ietf** | **van-jacobson**}

no iphc-profile *profile-name*

Syntax Description

profile-name	Name of the IPHC profile to be created or attached. The IPHC profile name can be a maximum of 32 characters. The name may not include quotation marks, white space, or special characters.
ietf	Specifies that the IPHC profile is for Internet Engineering Task Force (IETF) header compression.
van-jacobson	Specifies that the IPHC profile is for Van Jacobson header compression.

Command Default

No IPHC profile is created or attached.

Command Modes

Global configuration (to create an IPHC profile) Interface configuration (to attach an existing IPHC profile to an interface or subinterface)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **iphc-profile** command creates an IPHC profile used for enabling header compression and enters IPHC-profile configuration mode (config-iphcp). An IPHC profile is a template within which you can configure the type of header compression that you want to use, enable any optional features and settings for header compression, and then apply the profile to an interface, a subinterface, or a Frame Relay permanent virtual circuit (PVC).

Specifying the IPHC Profile Type

When you create an IPHC profile, you must specify the IPHC profile type by using either the **ietf** keyword or the **van-jacobson** keyword. The IETF profile type conforms to and supports the standards established with RFC 2507, RFC 2508, RFC 3544, and RFC 3545 and is typically associated with non-TCP header compression (for example, RTP header compression). The Van Jacobson profile type conforms to and supports the standards established with RFC 1144 and is typically associated with TCP header compression.

Note If you are using Frame Relay encapsulation, you must specify the **ietf**keyword (not the **van-jacobson** keyword).

Considerations When Specifying the IPHC Profile Type

When specifying the IPHC profile type, consider whether you are compressing TCP traffic or non-TCP traffic (that is, RTP traffic). Also consider the header compression format capabilities of the remote network link that will receive traffic. The IPHC profile type that you specify directly affects the header compression format used on the remote network links to which the IPHC profile is applied. *Only* TCP traffic is compressed on remote network links using a Van Jacobson IPHC profile, whereas TCP *and/or* non-TCP traffic (for example, RTP traffic) is compressed on remote network links using an IETF IPHC profile.

Note The header compression format in use on the router that you are configuring and the header compression format in use on the remote network link must match.

Configurable Header Compression Features and Settings

The specific set of header compression features and settings that you can configure (that is, enable or modify) is determined by the IPHC profile type that you specify (either IETF or Van Jacobson) when you create the IPHC profile. Both sets are listed below.

If you specify Van Jacobson as the IPHC profile type, you can enable TCP header compression and set the number of TCP contexts. The table below lists each available Van Jacobson IPHC profile type header compression feature and setting and the command used to enable it.

Table 1 Van Jacobson IPHC Profile Type Header Compression Features and Settings

Command	Feature or Setting
tcp	Enables TCP header compression.
tcp contexts	Sets the number of contexts available for TCP header compression.

If you specify IETF as the IPHC profile type, you can enable non-TCP header compression (that is, RTP header compression), along with a number of additional features and settings. The table below lists each available IETF IPHC profile type header compression feature and setting and the command or commands used to enable it.

Table 2 IETF IPHC Profile Type Header Compression Features and Settings

Command	Feature or Setting
feedback	Enables the context-status feedback messages from the interface or link.

Command	Feature or Setting
maximum header	Sets the maximum size of the compressed IP header.
non-tcp	Enables non-TCP header compression.
non-tcp contexts	Sets the number of contexts available for non-TCP header compression.
rtp	Enables RTP header compression.
recoverable-loss	Enables Enhanced Compressed Real-Time Transport Protocol (ECRTP) on an interface.
refresh max-period refresh max-time refresh rtp	Sets the context refresh (full-header refresh) options, such as the amount of time to wait before a full header is refreshed.
tcp	Enables TCP header compression.
tcp contexts	Sets the number of contexts available for TCP header compression.

For More Information About IPHC Profiles

For more information about using IPHC profiles to configure header compression, see the “Header Compression” module and the “Configuring Header Compression Using IPHC Profiles” module of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4T.

Examples

In the following example, an IPHC profile called profile1 is created, and the Van Jacobson IPHC profile type is specified.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile1 van-jacobson
Router(config-iphcp)# end
```

In the following example, a second IPHC profile called profile2 is created. For this IPHC profile, the IETF IPHC profile type is specified.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# end
```

In the following example, an existing IPHC profile called profile2 is attached to serial interface 3/0. For this IPHC profile, the IPHC profile type (in this case, IETF) of profile2 is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface serial 3/0
Router(config-if)# iphc-profile profile2 ietf
Router(config-iphcp)# end
```

Related Commands

Command	Description
feedback	Enables the context-status feedback messages from the interface or link.
maximum header	Specifies the maximum size of the compressed IP header.
non-tcp	Enables non-TCP header compression within an IPHC profile.
non-tcp contexts	Sets the number of contexts available for non-TCP header compression.
recoverable-loss	Enables ECRTP on an interface.
refresh max-period	Sets the number of packets sent between full-header refresh occurrences.
refresh max-time	Sets the amount of time to wait before a full-header refresh occurrence.
refresh rtp	Enables a context refresh occurrence for RTP header compression.
rtp	Enables RTP header compression within an IPHC profile.
show iphc-profile	Displays configuration information for one or more IPHC profiles.
tcp	Enables TCP header compression within an IPHC profile.
tcp contexts	Set the number of contexts available for TCP header compression.

lane client qos

To apply a LAN Emulation (LANE) quality of service (QoS) database to an interface, use the **laneclient** qos command in subinterface configuration mode. To remove the QoS over LANE feature from the interface, use the **no** form of this command.

lane client qos *database-name*

no lane client qos *database-name*

Syntax Description

database-name	Name of the QoS database.

Command Default

This command is not configured by default.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

This example shows how to apply a LANE QoS database to a subinterface:

```
Router(config-subif)# lane client qos user1
```

Related Commands

Command	Description
atm-address	Specifies the QoS parameters associated with a particular ATM address.
lane qos database	Begins the process of building a QoS over LANE database
show lane qos database	Displays the contents of a specific QoS over LANE database.
ubr+ cos	Maps a CoS value to a UBR+ VCC.

lane qos database

To build the LAN Emulation (LANE) quality-of-service database, use the **laneqosdatabase**command in global configuration mode. To remove a LANE QoS database name, use the **no** form of this command.

lane qos database *name*

no lane qos database *name*

Syntax Description

name	Name of the LANE QoS database.

Command Default

This command is not configured by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command specifies a named database of QoS parameters. The database can be applied on the subinterfaces on which a LANE client is configured.

Examples

This example shows how to begin configuring a QoS over LANE database named user1 on a Catalyst 5000 family ATM switch:

```
ATM# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ATM(config)# lane qos database user1
```

This example shows how to begin configuring a QoS over LANE database named user2 on a router:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# lane qos database user2
```

Related Commands

Command	Description
atm-address	Specifies the QoS parameters associated with a particular ATM address.
lane client qos	Applies a QoS over LANE database to an interface.
show lane qos database	Displays the contents of a specific QoS over LANE database.
ubr+ cos	Maps a CoS value to a UBR+ VCC.

load protocol

To load a protocol header description file (PHDF) onto a router, use the **loadprotocol**command in global configuration mode. To unload all protocols from a specified location or a single protocol, use the **no** form of this command.

load protocol *location* **:** *filename*

no load protocol {*location* **:** *filename* | *protocol-name*}

Syntax Description

location **:** *filename*	Location of the PHDF that is to be loaded onto the router. When used with the no version of this command, all protocols loaded from the specified filename will be unloaded. **Note** The location must be local to the router.
protocol-name	Unloads only the specified protocol. **Note** If you attempt to unload a protocol that is being referenced by a filter, you will receive an error.

Command Default

If this command is not issued, no PHDFs will be loaded onto the router.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

Flexible packet matching allows users to classify traffic on the basis of any portion of a packet header given the protocol field, length, and pattern. Protocol headers are defined in separate files called PHDFs; the field names that are defined within the PHDFs are used for defining the packet filters. A PHDF is a file that allows the user to leverage the flexibility of extensible markup language (XML) to describe almost any protocol header. The important components of the PHDF are the version, the XML file schema location, and the protocol field definitions. The protocol field definitions name the appropriate field in the protocol header, allow for a comment describing the field, provide the location of the protocol header field in the header (the offset is relative to the start of the protocol header), and provide the length of the field. Users can choose to specify the measurement in bytes or in bits.

Note The total length of the header must be specified at the end of each PHDF.

In case of a redundant setup, users should ensure all PHDFs that are used in the flexible packet matching configuration are present on the corresponding standby disk. If the PHDFs are not on standby disk, all flexible packet matching policies using the PHDFs will be broken.

Users can write their own custom PHDFs via XML. However, the following standard PHDFs can also be loaded onto the router: ip.phdf, ether.phdf, tcp.phdf, and udp.phdf.

Standard PHDFs are available on Cisco.com at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/fpm

Because PHDFs are defined via XML, they are not shown in a running configuration.

Issue the **loadprotocol** command to apply filters to a protocol by defining and loading a PHDF for that protocol header.

Examples

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

The following example is the XML setup for the PHDF “ip.phdf:”

```
<?xml version="1.0" encoding="UTF-8"?>
<phdf xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchem
aLocation="D:\harinadh\Doc\Projects\FPME\XML\ex.xsd">
<protocol name="ip" description="Definition-for-the-IP-protocol">
<field name="version" description="IP-version">
<offset type="fixed-offset" units="bits"> 0 </offset>
<length type="fixed" units="bits">4</length>
</field>
<field name="ihl" description="IP-Header-Length">
<offset type="fixed-offset" units="bits">4</offset>
<length type="fixed" units="bits">4</length>
</field>
<field name="tos" description="IP-Type-of-Service">
<offset type="fixed-offset" units="bits">8</offset>
<length units="bits" type="fixed">8</length>
</field>
<field name="length" description="IP-Total-Length">
<offset type="fixed-offset" units="bytes">2</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="identification" description="IP-Identification">
<offset type="fixed-offset" units="bytes">4</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="flags" description="IP-Fragmentation-Flags">
<offset type="fixed-offset" units="bytes">6</offset>
<length type="fixed" units="bits">3</length>
</field>
<field name="fragment-offset" description="IP-Fragmentation-Offset”>
<offset type="fixed-offset" units="bits">51</offset>
<length type="fixed" units="bits">13</length>
</field>
<field name="ttl" description="Definition-for-the-IP-TTL">
<offset type="fixed-offset" units="bytes">8</offset>
<length type="fixed" units="bytes">1</length>
</field>
<field name="protocol" description="IP-Protocol">
<offset type="fixed-offset" units="bytes">9</offset>
<length type="fixed" units="bytes">1</length>
</field>
<field name="checksum" description="IP-Header-Checksum">
<offset type="fixed-offset" units="bytes">10</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="source-addr" description="IP-Source-Address">
<offset type="fixed-offset" units="bytes">12</offset>
<length type="fixed" units="bytes">4</length>
</field>
<field name="dest-addr" description="IP-Destination-Address">
<offset type="fixed-offset" units="bytes">16</offset>
<length type="fixed" units="bytes">4</length>
</field>
<headerlength type="fixed" value="20"></headerlength>
</protocol>
</phdf>
```